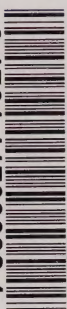



3 1761 11709038 1









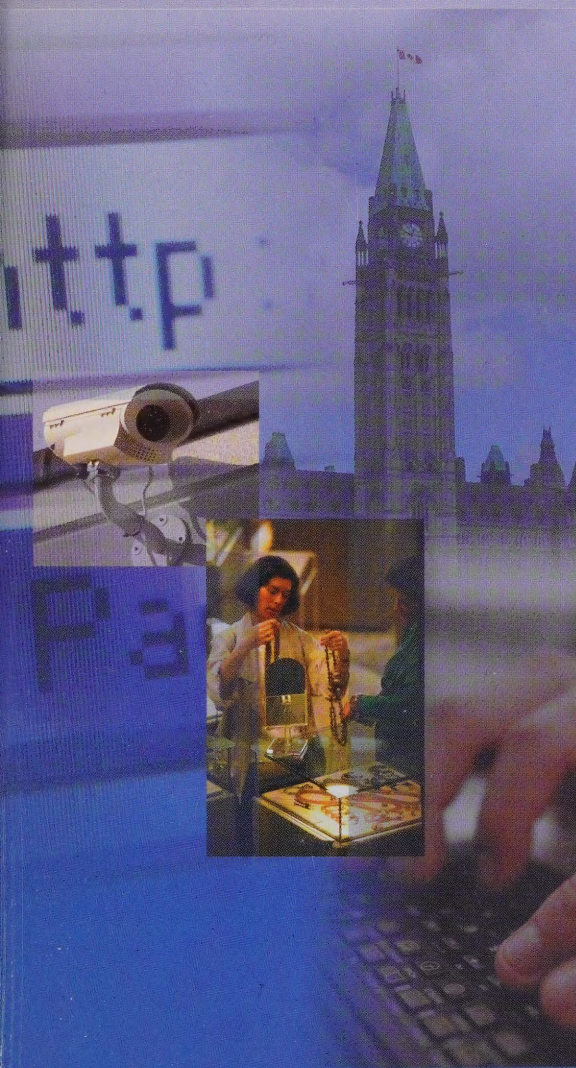
Digitized by the Internet Archive  
in 2023 with funding from  
University of Toronto

<https://archive.org/details/31761117090381>





# Privacy



## Annual Report to Parliament 2004

Report on the  
*Personal Information  
Protection and  
Electronic Documents Act*



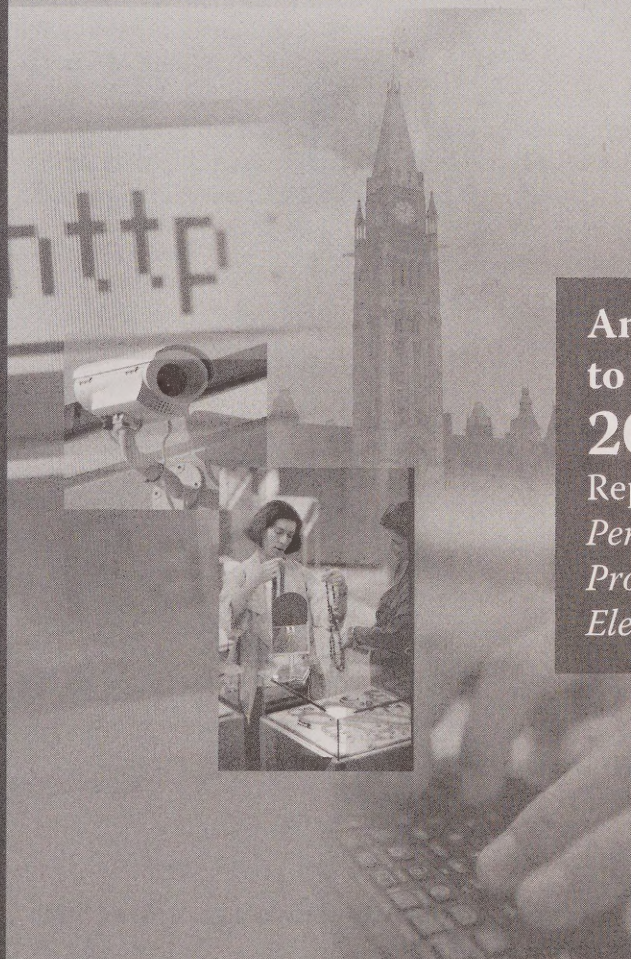


Privacy Commissioner  
of Canada



Commissaire à la protection  
de la vie privée du Canada

# Privacy



## **Annual Report to Parliament 2004**

*Report on the  
Personal Information  
Protection and  
Electronic Documents Act*

Canada





Office of the Privacy Commissioner of Canada  
112 Kent Street  
Ottawa, Ontario  
K1A 1H3

(613) 995-8210, 1-800-282-1376  
Fax (613) 947-6850  
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2005  
Cat. No. IP51-1/2005  
ISBN 0-662-68986-0

This publication is also available on our Web site at [www.privcom.gc.ca](http://www.privcom.gc.ca), in addition to our 2004-2005 Annual Report on the *Privacy Act*.



**Privacy Commissioner  
of Canada**

112 Kent Street  
Ottawa, Ontario  
K1A 1H3  
Tel.: (613) 995-8210  
Fax: (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca

**Commissaire à la protection  
de la vie privée du Canada**

112, rue Kent  
Ottawa (Ontario)  
K1A 1H3  
Tél. : (613) 995-8210  
Téléc. : (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca



October 2005

The Honourable Daniel Hays, Senator  
The Speaker  
The Senate of Canada  
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2004.

Yours sincerely,

A handwritten signature in cursive script that reads "Jennifer Stoddart".  
Jennifer Stoddart  
Privacy Commissioner of Canada





**Privacy Commissioner  
of Canada**

112 Kent Street  
Ottawa, Ontario  
K1A 1H3  
Tel.: (613) 995-8210  
Fax: (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca

**Commissaire à la protection  
de la vie privée du Canada**

112, rue Kent  
Ottawa (Ontario)  
K1A 1H3  
Tél. : (613) 995-8210  
Télec. : (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca



October 2005

The Honourable Peter Milliken, M.P.  
The Speaker  
The House of Commons  
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2004.

Yours sincerely,

A handwritten signature in dark ink that reads "Jennifer Stoddart".

Jennifer Stoddart  
Privacy Commissioner of Canada





# Table of Contents

---

**Foreword .....1**

**Our Multi-Faceted Mandate .....7**

**Policy Perspective.....9**

    Technology .....9

    Parliament’s Window on Privacy.....10

    National Security .....13

    Outsourcing and Transborder Flows of Personal Information .....16

**Research into Emerging Privacy Issues .....19**

**Substantially Similar Provincial Legislation.....21**

    Jurisdictional Issues .....23

**Evolution of the *Personal Information Protection and Electronic Documents Act* .....29**

    Statutory Changes .....29

    2006 Review of *PIPEDA* by Parliament .....30

---

<b>Complaints.....</b>	<b>33</b>
Investigation Process under <i>PIPEDA</i> .....	38
Definitions of Findings under <i>PIPEDA</i> .....	40
Inquiries.....	41
Select Cases under <i>PIPEDA</i> .....	43
Select Settled Cases under <i>PIPEDA</i> .....	58
Incidents under <i>PIPEDA</i> .....	66
Following Up on <i>PIPEDA</i> Case Investigations .....	71
 <b>Audit and Review .....</b>	 <b>75</b>
Strengthening the Audit Function .....	75
Keeping Watch on Radio Frequency Identification.....	76
 <b>In the Courts .....</b>	 <b>79</b>
<i>PIPEDA</i> Applications.....	79
Judicial Review .....	87
 <b>Public Education and Communications .....</b>	 <b>91</b>
 <b>Corporate Services .....</b>	 <b>95</b>
On the Path to Institutional Renewal.....	95
Financial Information.....	99

---

# Foreword

---



The year 2004 saw the *Personal Information Protection and Electronic Documents Act (PIPEDA)* reach maturity, with the Act extending across the country to all commercial activities, except in provinces with legislation deemed substantially similar. British Columbia, Alberta and Quebec have enacted private sector privacy legislation that has been deemed substantially similar to *PIPEDA*. *PIPEDA* applies to federal works, undertakings and businesses across the country, as well as to interprovincial and international transactions.

The maturing of *PIPEDA* is cause for some celebration. Canadians now have comprehensive rights relating to personal information in the private sector in Canada, in addition to longstanding protections in the public sector through the *Privacy Act* and its provincial equivalent legislation. That is not to say that either the private sector or public sector privacy laws fully protect the privacy rights of Canadians in every sense. They do not. But much of the essential framework for protecting those rights is now in place. Our Office will continue to enforce and analyze the application of *PIPEDA* to ensure that Canadians are well-served by it, and that the Canadian private sector understands and respects its obligations under the Act. We will continue to help the business community comply with it, and develop the best practices which will minimize burden and clarify expectations.

## Interjurisdictional challenges

As with any relatively new legislation, problems can emerge. Where a province has enacted legislation that is substantially similar to all or part of *PIPEDA*, confusion may arise about which law – provincial or federal – will apply to certain information-handling practices. In other cases, the laws of two jurisdictions may be involved in addressing an issue. Some elements of the handling of personal information may be subject to a provincial law – the collection of the information within a province,



for example – while another element, such as the transborder disclosure of the information, may fall under *PIPEDA*.

However, the dust is beginning to settle around these jurisdictional issues due to concerted efforts by our Office, our provincial counterparts and industry. We are working with our provincial colleagues to streamline investigations where provincial and federal jurisdictions both apply. It is not our intention to make life difficult for those who must comply with the various privacy laws in Canada, and we clearly do not want to waste the limited resources available to privacy commissioners across Canada by duplicating efforts in conducting investigations and developing policy.

### **A complex and changing universe**

There are many powerful forces in the universe in which we assert our privacy rights – galloping advances in surveillance and data-handling technologies, global competition in business which drives companies to obtain and use more personal information about customers and personnel, and the government imperative to acquire personal information to enhance administrative efficiency and respond to the security concerns of our world. Those of us attempting to protect this fundamental right must call out strongly for a debate that can be at times unpopular and demands a wealth of expertise in ever more complex fields of research. It is a challenge to keep up.

It is important to remember that information is power, and holding the personal information of individuals conveys power to the holder. One complexity that we have been grappling with this year stems from a convergence of two phenomena which are not new by any means, but which have reached a critical point. “Outsourcing” of data processing operations and call centres results in the personal information of Canadian residents or customers of Canadian companies being transferred and processed outside Canada. The thirst of foreign governments, particularly that of the United States and its allies in the war on terror, for access to personal information for “security” purposes means that the outsourced data may be accessed for law enforcement or national security purposes, outside our jurisdiction and the protection of our laws and our Court system.

Transborder data flow has been discussed in Canada since the 1960s. The original report on *Privacy and Computers*, published in 1972 by the Departments of Communications and Justice, dealt with the matter extensively, including matters of sovereignty. The issue prompted the Organization for Economic Cooperation and Development (OECD) to meet and develop the first Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data in 1980, and it drove

the European Union to pass its Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Yet we know very little about the details of transborder flows of personal information about Canadian residents and customers.

The current interest in the *USA PATRIOT Act* has raised an issue that has been lurking beneath the surface for decades – the extent to which Canadian businesses, and governments in Canada, should share personal information with foreign governments. The discussion is far from over. In fact, it is just beginning. Our Office endorsed many of the recommendations of the B.C. Information and Privacy Commissioner, David Loukidelis, on issues of transborder flows of personal information and we will continue working to ensure Canadians' privacy protections remain in place.

This Office is tasked with protecting privacy in Canada. We cannot do the job alone, we depend on all players in society to contribute to preserving the freedoms and rights which are an intrinsic part of Canada's rich fabric and history. The complexity of the current privacy environment has led our Office to launch a Contributions Program to help develop a national privacy research capacity in Canada. The findings of this first round of research projects will be available in 2005. These research findings will complement the existing policy research function within our Office, and in a modest way help to enrich the community of privacy scholarship in Canada.

### **Responding to a greater need**

This Office received 723 complaints under *PIPEDA* between January 1 and December 31, 2004, more than double the 302 received in the previous calendar year. We closed 379 complaints, significantly more than the 278 cases closed in 2003. While the debate about the merits of having the Commissioner continue to operate as an ombudsman versus giving the Commissioner order-making powers remains, it is clear that our Office has accomplished much that is positive using the current ombudsman approach. Some 40 per cent of the complaints closed during the year were settled, and another seven per cent resolved – an indication that suasion, a prominent feature of the ombudsman approach, is an effective tool.

We have introduced a formal procedure of systematic follow-ups to complaint investigations under *PIPEDA*. We will now be in position to monitor the progress of organizations in implementing commitments they make during complaint investigations and in response to the recommendations our Office issues to them. Equally important, our Audit and Review Branch is strengthening its capacity to audit organizations subject to *PIPEDA*.



We faced many challenges in 2004, challenges that will only increase in frequency and complexity. This is not a time for those concerned about this fundamental human right called privacy to shrink from speaking out, from debate or from controversy. We will seize the opportunity of the 2006 review of *PIPEDA* to make recommendations about how to improve and better enforce the two pieces of legislation that we oversee. Although the Act is still very new in application, the dynamic environment of information policy demands that we keep current and try to ensure that the legislation also responds effectively to current threats. We are developing a list of improvements and suggestions for change, and we are confident that in another five years, when the next review is due, there will be more changes necessary. Parliament was wise to insist on periodic review of this legislation, and we will continue to push for review of the *Privacy Act* and inclusion of such a review mechanism in it.

*This year, we have published two separate reports, dividing the Privacy Act from the Personal Information Protection and Electronic Documents Act (PIPEDA). We felt this was more appropriate given that the Privacy Act requires us to report on the fiscal year (2004–2005), while under PIPEDA we are required to report on the calendar year (2004). As well, each Act provides a separate framework for investigations and audits. Both our reports detail efforts we have taken to meet the growing demands on our Office to act as the guardians of privacy for Canadians on behalf of Parliament. There is much overlapping between these reports because many of our activities are not particular to one law or another and, increasingly, the policy issues are common across the two regimes.*





# Our Multi-Faceted Mandate

---

The Office of the Privacy Commissioner oversees two laws – the *Privacy Act*, which applies to federal government institutions, and *PIPEDA*, which governs personal information management in commercial activities.

Parliament requires our Office to ensure that both the federal public sector and private sector (in most provinces) are held accountable for their personal information handling, and that the public is informed about privacy rights. The mandate is not always well understood.

As an independent ombudsman, we are:

- An *investigator* and *auditor* with full powers to investigate and initiate complaints, conduct audits and verify compliance under both Acts;
- A *public educator* and *advocate* with a responsibility both to sensitize businesses about their obligations under *PIPEDA* and to help the public better understand their data protection rights;
- A *researcher* and *expert adviser* on privacy issues to Parliament, government and businesses; and
- An *advocate for privacy principles* involved in litigating the application and interpretation of the two privacy laws. We also analyze the legal and policy implications of bills and government proposals.





# Policy Perspective

---

In 2004, our major preoccupations in the policy area were the heightened demands for personal information in the name of national security, the transborder flow of personal information, and that hardy perennial, privacy invasive technologies. From cell phones in locker rooms to global positioning systems in cars, the need to measure the impact of these new technologies and read the privacy law into their design and application is an ongoing challenge.

## Technology

During the past year, the privacy implications of using Radio Frequency Identification Devices (RFIDs) as tracking devices have become increasingly prominent. RFIDs encompass technologies that use radio waves to read a serial number stored on a microchip. The microchip or tag can be placed in military equipment, passports, clothing, currency notes, vehicles, tires, pass cards and just about anything else sold in the marketplace, including food and drink packages. RFID applications include tracking goods from the manufacturer to the retail store, tracking people in a health institution or monitoring the movements of schoolchildren.

Depending on its individual design, an RFID can transmit information over long distances or only a few centimeters. It may hold no personal information or store extensive personal information, including biometrics. An RFID can be “active” or “passive” – active where it has its own power to broadcast information to a reader, or passive in that it lies dormant until awakened by a signal from a “reader.”

The combination of tags, (sometimes smaller than a grain of rice or built invisibly into the paper of a product), powerful coding and advanced computer systems has created enormous economic incentives for companies to introduce RFID technology.

A recent market forecast predicts that the global value of the total RFID tag market will expand from \$1.95 billion in 2005 to \$26.9 billion in 2015. Given that each RFID tag may eventually cost only pennies, the potential scale of use is greater than almost any other single technology.

Organizations must think carefully about the legal implications of deploying RFID systems. Amidst the flurry of activity involving RFIDs, very few people fully understand the myriad of privacy implications. We are now encountering many marketplace uses of RFIDs, and expect that we will soon be investigating complaints about tracking the use of RFIDs.

Similarly, although there have been some interesting stories in the press about the use and abuse of global positioning technology, most individuals are unaware of the data that is accumulated by such devices. Fortunately, *PIPEDA* contains an innovative provision requiring openness with respect to information practices.

Organizations placing global positioning devices in consumer goods or conveyances (rental cars, for example) must identify what the device does, the data it collects, how long the data is kept, and who has access to it.

We are entering a world where computing power will be present in the most ordinary day-to-day devices. If we are not careful, that power will be used to gather or broadcast personal information in ways that greatly diminish our privacy, not to mention our autonomy and human dignity. As transmitting devices are built into roadsides, licence plates, currency and books, we are hard pressed to keep up with the potential privacy invasions and abuses. Canadians need to become more aware of and participate in discussing the privacy issues that flow from these developments. We need to shape our future into something that reflects the rights and freedoms we cherish today. From Reginald Fessenden to Marshall McLuhan, Canadians have shown leadership in the development of communications technologies and in communications theory. We are confident we can now rise to the current challenge, and demonstrate how we can use these powerful devices, in the world of ubiquitous computing and communications, yet maintain respect for that most fundamental of human values, privacy.

## Parliament's Window on Privacy

The Privacy Commissioner of Canada is an Agent of Parliament who reports directly to the Senate and the House of Commons. As such, the OPC acts as Parliament's window on privacy issues. Through the Commissioner, Assistant Commissioners and



other senior OPC staff, the Office brings to the attention of Parliamentarians issues that have an impact on the privacy rights of Canadians. The OPC does this by tabling Annual Reports to Parliament, by appearing before Committees of the Senate and the House of Commons to comment on the privacy implications of proposed legislation and government initiatives, and by identifying and analyzing issues that we believe should be brought to Parliament's attention.

The Office also assists Parliament in becoming better informed about privacy, acting as a resource or centre of expertise on privacy issues. This includes responding to a significant number of inquiries and letters from Senators and Members of Parliament.

➤ *Appearances before Parliamentary Committees*

Appearances before committees of the Senate and the House of Commons constitute a key element of our work as Parliament's window on privacy issues. During the period covered by this report, the Privacy Commissioner and other senior OPC staff appeared nine times before Parliamentary committees: six times on bills with privacy implications and three times on matters relating to the management and operations of the Office.

The OPC appeared on the following bills before Parliamentary committees in 2004:

- Bill C-6, the *Assisted Human Reproduction Act* (March 3, 2004)
- Bill C-7, the *Public Safety Act, 2002* (March 18, 2004)
- Bill C-2, *An Act to Amend the Radiocommunication Act* (May 6, 2004)
- Bill C-12, the *Quarantine Act* (November 18, 2004)
- Bill C-22, *An Act to establish the Department of Social Development and to amend and repeal certain related Acts* (December 9, 2004)
- Bill C-23, *An Act to establish the Department of Human Resources and Skills Development and to amend and repeal certain related Acts* (December 9, 2004)
- Bill C-11, the *Public Servants Disclosure Protection Act* (December 14, 2004)

Regarding the management and operations of the Office, OPC officials appeared before Parliamentary committees on the following matters in 2004:

- Annual Report and Main Estimates 2003-2004 (November 17, 2004)
- Supplementary Estimates (December 1, 2004)

► *Other Parliamentary Liaison Activities*

The OPC has undertaken a number of other initiatives over the course of the past year to improve its ability to advise Parliament on privacy matters.

In May 2004, we created a dedicated Parliamentary liaison function within the Office to improve our relationship with Parliament. This function resides in the Research and Policy Branch, reflecting the OPC's desire to focus its Parliamentary affairs activities on providing in-depth and accurate policy advice to Senators and Members of Parliament.

Improving on how we assess, monitor and forecast Parliamentary activity has been a priority for us in the past year. The OPC put in place a new and improved system for monitoring the status of bills on Parliament Hill, as well as keeping tabs on new and emerging developments of interest to privacy promotion and protection. Our goal is to build bridges to departments so that we can comment earlier in the legislative process, when our criticisms could be dealt with more effectively. It is often too late when a bill has been introduced in the House of Commons, to rethink approaches to information issues.

The Office has responded to a significant number of inquiries and letters from Senators and MPs this year, and the Commissioner and Assistant Commissioners have also met privately with Senators and MPs who wished to discuss policy matters relating to privacy, or wanted to know more about the operations of the Office.

In late 2004, the OPC in conjunction with the Office of the Information Commissioner, and in collaboration with the Research Branch of the Library of Parliament, held an information session for Parliamentarians and their staff on the roles and mandates of both Offices. This information session was well attended and raised many questions among participants. We believe such information sessions contribute to increasing awareness of privacy issues on Parliament Hill, and look forward to holding more such sessions in the future.

► *Priorities for the Coming Year*

The Office expects to be busy in the area of Parliamentary affairs over the next fiscal year. There are a number of bills of interest to us expected in the upcoming session, and the statutory review by Parliament of the *Personal Information Protection and Electronic Documents Act* is expected to start in 2006. The OPC plans to play a

constructive role during this review, by providing thoughtful advice to Parliamentarians mandated with studying at how the Act has worked over the course of its first years of implementation, and how it may be modified and improved.

The OPC will continue to follow with interest the Parliamentary review of the *Anti-terrorism Act*. The Privacy Commissioner appeared twice before committee on this matter in fiscal year 2005-06—once before a Senate special committee reviewing the Act (May 9, 2005), and on another occasion before a sub-committee of the Commons Standing Committee on Justice (June 1, 2005).

We recognize that to act as an effective Agent of Parliament we need to have good working relationships with federal departments and agencies. The OPC plans to put more emphasis on identifying and raising privacy concerns when government initiatives are being developed rather than waiting until they reach Parliament, as this increases the possibility that privacy concerns will be taken into account.

## National Security

In May 2004, the *Public Safety Act, 2002* was enacted. The Act, first introduced in November 2001 in the wake of the September 11 terrorist attacks, allows the Minister of Transport, the Commissioner of the RCMP and the Director of the Canadian Security Intelligence Service (CSIS), without a warrant, to compel air carriers and operators of aviation reservation systems to provide information about passengers. While this may seem reasonable given the risks that terrorists pose to air transport, authorities are not using this information exclusively for anti-terrorism and transportation safety. The *Public Safety Act, 2002* also allows the information to be used to identify passengers for whom there are outstanding arrest warrants for a wide range of lesser criminal offences. In other words, the machinery of anti-terrorism is being used to meet the needs of ordinary law enforcement, lowering the legal standards that law enforcement authorities in a democratic society must normally meet.

The retention and mining of private sector data collections by government sends a troubling signal to private sector organizations trying to comply with privacy legislation. If the government can use data to manage risks from unknown individuals, why can't the private sector? Private sector companies are cutting down on data collection to comply with *PIPEDA*, but now the government is asking them to retain it so that they can access it for government purposes. *PIPEDA* sets a high bar for organizations with respect to using and disclosing personal information without consent for the purposes of investigating fraud and other illegal activities that have



an impact, while the standards that government must meet under the *Privacy Act* are much less rigorous.

In 2004, our Office raised concerns about a provision in the *Public Safety Act, 2002* that amends *PIPEDA*. The amendment allows organizations subject to *PIPEDA* to collect personal information, without consent, for the purposes of disclosing this information to government, law enforcement and national security agencies if the information relates to national security, the defence of Canada or the conduct of international affairs. Allowing private sector organizations to collect personal information without consent in these circumstances effectively co-opts them into service for law enforcement activities. This dangerously blurs the line between the private sector and the state. We comment more extensively on public safety issues in the *Privacy Act* Annual Report, but this is also an important issue under *PIPEDA* because of the potential for inappropriate manipulation of private sector data to serve state interests.

The 2001 *Anti-terrorism Act* contained a provision requiring a review after three years. The Senate has appointed a special committee to conduct its review. The House of Commons review is being conducted by the Subcommittee on Public Safety and National Security, a subcommittee of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness. However, the Commons Committee is not looking at the many other pieces of legislation that were also enacted or amended in the wake of the terrorist attacks. Many of these laws contain extensive powers to intrude and should be examined as well.

The *Official Secrets Act* was replaced by the *Security of Information Act* in 2001. Section 10 of the new Act allows the deputy head of a department, on the issuance of a certificate, to bind members of the private sector to secrecy for life with respect to methods of investigation or special operations. We understand that sometimes it is necessary to deal with threats to our national security and critical infrastructure, but we raise the warning flag when we see new powers without complementary oversight provisions to ensure accountability. We have raised the issue of accountability and oversight in our submission to Parliament on the review of the *Anti-terrorism Act*, but this particular provision is in the *Security of Information Act*, and we think it merits public reporting on how often it is being used.

In the war on terror, governments have made it clear that they must have the cooperation of the private sector to ensure public safety and the security of the critical infrastructure. From the perspective of this Office, we must also ask whether we can

effectively oversee the private sector and the role it might play in security matters. In the United States, the use of private sector databases and information retention for law enforcement and anti-terrorism continue to attract criticism. We do not know the extent to which such use and retention occurs in Canada, but it is an issue of growing concern to Canadians and we are trying to get answers so that we can respond to their queries and complaints.

In July 2004, Canada began enforcing new marine security requirements under the International Maritime Organization's International Ship and Port Facility Security (ISPS) Code. To further enhance port security, Transport Canada is proposing to introduce a controversial Marine Facilities Restricted Area Access Clearance Program to screen port workers who have access to restricted areas. This screening process will involve collecting significant amounts of personal and potentially sensitive information about as many as 30,000 port workers. Once again, the extent to which such security checks are dependent on private sector information databases is of interest to our Office.

The issue of data-matching is an old one that has pre-occupied privacy scholars and oversight bodies for over twenty years. Technology has advanced, and we really no longer speak of data-matching but rather data-mining. There are many invisible uses of integrated information systems that collect and analyze significant amounts of personal information related to our travel patterns, our financial transactions, and even the people with whom we associate. Many of these systems would be viewed by consumers as immensely positive, were they to know of them and fully understand them because they provide faster loan approvals, instant recognition of credit card theft, and better customer service. However, these systems also now analyze deep reservoirs of personal information in an attempt to find patterns that might suggest that an individual is a security threat, a money launderer or is engaged in financing a terrorist group.

As law enforcement and national security agencies collect more information from more sources about more individuals, the chances increase that decisions will be based on information of questionable accuracy, or that information will be taken out of context.

When personal information is misused, misinterpreted or inappropriately disclosed it can have serious adverse consequences for individuals, families, and even communities. The problem is aggravated when, because of secrecy provisions and a lack of transparency, we cannot find out where the system broke down or on what basis individuals were wrongly targeted.

## Outsourcing and Transborder Flows of Personal Information

The transfer of personal information from Canada into foreign jurisdictions (transborder data flows) is another issue as old as privacy legislation itself. Scholars and government policy experts in the 1960s and 70s anticipated greater flows of data in the future as communications technology improved. Whether they could have predicted the enormity of the global flow of data that we see today is another question.

In 2004, the transborder issue became more visible in Canada when a complaint was raised in British Columbia about the outsourcing of health information processing from the B.C. government to a U.S.-linked company operating in the province. The B.C. Government Employees Union alleged that the information would be available to the U.S. government under the expansive search powers introduced in 2001 by the *USA PATRIOT Act*. Although there have been many high profile instances of outsourcing in recent years, with occasional concern about the privacy implications, this appeared to be the first where a specific piece of legislation was singled out as a threat. The B.C. Information and Privacy Commissioner, David Loukidelis, took the step of issuing a call for public comment on this issue, and we submitted a brief in response.

Our submission explained that a company holding personal information *in Canada* about Canadian residents was not required to provide the information to a foreign government or agency in response to a direct court order issued abroad. In fact, the organization in Canada would in many cases violate *PIPEDA* if it disclosed the information without the consent of the individuals to whom the information relates.

However, there would be no violation of *PIPEDA*, for example, if the organization disclosed the information under Canadian legislation such as the *Aeronautics Act* provision that allows Canadian air carriers to disclose passenger information to foreign states.

We also concluded that an organization operating in a foreign country and that holds personal information about Canadians *in that country* must comply with the laws of that country. This means that when a Canadian organization outsources the processing of personal information to a company in the United States or another country, that information may be accessible under the laws of those countries.



The foreign government could of course request the same information through a mutual legal assistance treaty (MLAT) and ask the federal Department of Justice to arrange for Canadian law enforcement agencies to obtain the information from corporations in Canada for them – a system of government-to-government cooperation that predates the *USA PATRIOT Act*.

*PIPEDA* deals succinctly with transborder data flows in Principle 4.1.3 of the Schedule to the Act. This principle requires that information transferred for processing must be protected at a level “comparable” to that provided by *PIPEDA*. However, when data is held or processed outside Canada there is a loss of control over what a foreign jurisdiction might do with that information and our Office has no oversight authority.

We urgently need to address these flows of personal information so that we can ensure protection of the personal information we send around the world. A series of news reports in early 2005 concerning security breaches by companies in other countries holding personal information about Canadians has further emphasized the importance of devoting attention to transborder flows of personal information.



## Research into Emerging Privacy Issues

**O**n June 1, 2004, our Office officially launched a Contributions Program to support research by not-for-profit groups, including education institutions, industry and trade associations, and consumer, voluntary and advocacy organizations, into the protection of personal information and the ways to protect it. The program represented a milestone in the development of national privacy research capacity in Canada. The program is designed to assist our Office to foster greater public awareness and understanding of privacy.

The 2003-2004 Contributions Program had two key priorities. The first was to examine how and to what extent emerging technologies affect privacy. These included video surveillance, RFIDs, location technology and biometrics. Many of these technologies have their most profound impact on privacy when they are in the hands of government, but they often also have significant privacy implications when used by the private sector.

The second priority of the research program related more directly to the implementation of *PIPEDA*, especially since new sectors of the economy became subject to the Act in January 2004. This part of the Contributions Program focused on awareness and promotion of good privacy practices as a key component of responsible commercial behaviour.



The projects that were funded for a total of \$371,590 include:

### FUNDED PROJECTS

<u>Canadian Marketing Association</u> <b>Toronto, Ontario</b>	<b>Taking Privacy to the Next Level</b> <i>Assess and develop privacy best practices to assist businesses in better handling customer personal information under PIPEDA</i>	\$50,000
<u>École nationale d'administration publique (ENAP)</u> <b>Quebec, Quebec</b>	<b>Study on the use of video surveillance cameras in Canada</b> <i>Perceptions, issues, privacy impact and best practices on the use of video surveillance</i>	\$50,000
<u>Queen's University</u> <b>Kingston, Ontario</b>	<b>Location Technologies: Mobility, Surveillance and Privacy</b> <i>Trends and stated and implicit purposes of technology with workers, consumers, travelers and citizens</i>	\$49,972
<u>The B.C. Freedom of Information and Privacy Association</u> <b>Vancouver, British Columbia</b>	<b>PIPEDA &amp; Identify Theft: Solutions for Protecting Canadians</b> <i>Gap analysis on weaknesses in personal information management practices that lead to identity theft and policy recommendations for PIPEDA implementation</i>	\$49,775
<u>Universities of Alberta and Victoria</u> <b>Edmonton, Alberta</b> <b>Victoria, British Columbia</b>	<b>Electronic Health Records and PIPEDA</b> <i>Implementation of PIPEDA in the health care sector and application to electronic health records in the primary care setting</i>	\$49,600
<u>University of Toronto</u> <b>Toronto, Ontario</b>	<b>A review of Internet privacy statements and on-line practices</b> <i>Evaluation of implementation of PIPEDA and privacy statements on the Internet by companies in the telecommunications, airline, banking and retail sectors</i>	\$48,300
<u>University of Victoria</u> <b>Victoria, British Columbia</b>	<b>Location-Based Services: An Analysis of Privacy Implications in the Canadian Context</b> <i>Privacy implications of geographic location-based services — issues raised and major challenges and guidance to encourage compliance</i>	\$27,390
<u>Option Consommateurs</u> <b>Montreal, Quebec</b>	<b>The challenge of consumer identification with new methods of electronic payment</b> <i>Current and new proposed methods of identification of consumers for electronic payment and risk factors</i>	\$17,100
<u>Simon Fraser University</u> <b>Vancouver, British Columbia</b>	<b>Privacy Rights and Prepaid Communications Services: Assessing the Anonymity Question</b> <i>Justification and feasibility of regulatory measures to eliminate the sale of anonymous prepaid communications services in Canada</i>	\$14,850
<u>Dalhousie University</u> <b>Halifax, Nova Scotia</b>	<b>An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies</b> <i>Study of RFID technology and privacy impact and legal measures to protect privacy</i>	\$14,603

The projects are to be completed in 2005. We will post links to the research results on our Web site.

# Substantially Similar Provincial Legislation

---

**O**ur Office is required by section 25(1) of *PIPEDA* to report annually to Parliament on the extent to which the provinces have enacted legislation that is substantially similar to *PIPEDA*.

Beginning on January 1, 2004, *PIPEDA* extended to all commercial activities. However, section 26(2)(b) allows the Governor in Council to issue an order exempting certain activities from the ambit of *PIPEDA*. This order can be issued if the province has passed legislation that is deemed substantially similar to *PIPEDA*. The order can exempt an organization, a class of organizations, an activity or a class of activities from the application of *PIPEDA* with respect to the collection, use or disclosure of personal information subject to that legislation that occurs within the province.

The intent of this provision is to allow provinces and territories to regulate the personal information management practices of organizations within their borders while ensuring seamless and meaningful privacy protection throughout Canada.

If the Governor in Council issues an Order declaring a provincial act to be substantially similar, the collection, use or disclosure of personal information by organizations subject to the provincial act will not be covered by *PIPEDA*. Interprovincial and international transactions will be subject to *PIPEDA*, and *PIPEDA* will continue to apply within a province to the activities of federal works, undertakings and businesses that are under federal jurisdiction, such as banks, airlines, and broadcasting and telecommunications companies.

### **Process for assessing provincial and territorial legislation**

On August 3, 2002, Industry Canada published a notice in the *Canada Gazette* Part 1 setting out how it will determine whether provincial/territorial legislation is deemed substantially similar to *PIPEDA*.

A province, territory or organization triggers the process by advising the Minister of Industry of legislation that they believe is substantially similar to *PIPEDA*. The Minister may also act on his or her own initiative and recommend to the Governor in Council that provincial or territorial legislation be found substantially similar. The notice states that the Minister will seek the Privacy Commissioner's views and include those views in the submission to the Governor in Council. The public and interested parties will also have a chance to comment.

According to the *Canada Gazette* notice, the Minister will expect substantially similar provincial or territorial legislation to:

- Incorporate the ten principles found in Schedule 1 of *PIPEDA*;
- Provide for an independent and effective oversight and redress mechanism, with powers to investigate; and
- Restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.

### **"Substantially similar" provincial legislation enacted to date**

Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector* came into effect, with a few exceptions, on January 1, 1994. The legislation sets out detailed provisions that enlarge upon and give effect to the information privacy rights contained in Articles 35 to 41 of the *Civil Code of Quebec*. In November 2003, the Governor in Council issued an Order in Council (P.C. 2003-1842, 19 November 2003) exempting organizations in that province, to which the provincial legislation applies. *PIPEDA* continues to apply to federal works, undertakings or businesses and to interprovincial and international transactions.

British Columbia and Alberta passed legislation in 2003 that applies to all organizations within the two provinces, except for (a) those covered by other provincial privacy legislation and (b) federal works, undertakings or businesses covered by *PIPEDA*. The two laws – both called the *Personal Information Protection Act* – came into force on January 1, 2004.

Using the criteria set out in the *Canada Gazette* notice – the presence of the ten principles found in Schedule 1 of *PIPEDA*, independent oversight and redress and a provision restricting collection, use and disclosure to legitimate purposes (a reasonable person test) – we concluded that the British Columbia and Alberta laws are substantially similar to *PIPEDA*.

For Alberta and British Columbia, the Governor in Council issued two Orders in Council (P.C. 2004-1163, 12 October 2004 and P.C. 2004-1164, 12 October 2004) exempting organizations, to which the provincial legislation applies. *PIPEDA* continues to apply to federal works, undertakings or businesses and to interprovincial and international transactions..

Ontario's *Personal Health Information Protection Act (PHIPA)* came into force on November 1, 2004. *PHIPA* establishes rules for the collection, use and disclosure of personal health information by health information custodians in Ontario. Our Office has informed Industry Canada that we believe *PHIPA* as it relates to health information custodians to be substantially similar to *PIPEDA*. Industry Canada has requested comments on a proposed order declaring the Ontario law substantially similar to *PIPEDA*, but an Order in Council had not been issued when we prepared this Annual Report.

## Jurisdictional Issues

For most of 2004 – beginning January 1 and ending October 12 – the Alberta and B.C. private sector privacy laws were in force, but had not yet been declared substantially similar to federal law. During this period, both the provincial private sector laws and *PIPEDA* applied. There was concurrent jurisdiction.

In Ontario, *PIPEDA* applied to personal information in the private sector (except for provincially-regulated employees) beginning on January 1, 2004. Ontario's *Personal Health Information Protection Act, 2004 (PHIPA)* came into force on November 1, 2004. Since November 1, both *PIPEDA* and the Ontario legislation have applied to personal health information in the private sector. As was the case with the Alberta and B.C. private sector legislation until Ontario's *PHIPA* is deemed substantially similar, both *PIPEDA* and *PHIPA* will apply to personal health information in the private sector.

Even a “substantially similar” order may not be broad enough to eliminate concurrent jurisdiction completely. With Ontario, for example, the “substantially similar” order



will not apply to some entities regulated by Ontario's *PHIPA*. The proposed order may apply in respect of the rules governing health information custodians; Ontario's *PHIPA* would therefore be the sole law applying to health information custodians' collection, use, or disclosure of personal information in Ontario.

But the substantially similar order would not apply to third parties who receive personal information from health information custodians. *PHIPA* imposes rules on non-health information custodians only about the use and disclosure of personal health information. *PHIPA* does not regulate other privacy obligations, such as collection, access and safeguards. Therefore, *PIPEDA* would continue to apply to these activities.

One simple way to avoid the work of Commissioners overlapping in areas of concurrent jurisdiction is to reach informal agreements about who handles what. Our Office will work closely with Ontario, as it has with B.C. and Alberta, to ensure that both Acts are enforced in the most seamless way possible.

Even where a "substantially similar" order exists, not all intraprovincial commercial activity will necessarily be covered by the order, and jurisdictional boundaries are not always clear. Complex jurisdictional issues may still arise and require close collaboration between jurisdictions to deal with them.

For instance, Alberta's *Health Information Act (HIA)* applies to health service providers who are paid under the Alberta Health Care Insurance Plan to provide health services. On this definition, *HIA* does not cover health practitioners, who provide health services privately. While Alberta's *Personal Information Protection Act (PIPA)* does apply to private sector organizations, it does not apply to health information, as defined by *HIA*, which is collected, used or disclosed for health care purposes. Under this regime, the collection, use or disclosure of personal health information by practitioners working in private practice to provide health services seems to have fallen between the cracks; it is not currently covered by either Alberta Act. Hence, such activity is subject to the federal *PIPEDA*.

As a postscript, a bill was introduced in the Legislative Assembly of Alberta in March 2005 to amend Alberta's *PIPA* in favour of bringing the activities of private practitioners who collect, use or disclose personal health information in the course of providing health services clearly within the scope of *PIPA*. This amendment has since come into force and resolved this jurisdictional problem.

**Flows of personal information across provincial boundaries**

Another aspect of the jurisdictional issue arises with flows of information across provincial boundaries. An Alberta company may disclose personal information to another company in Saskatchewan in the course of a commercial activity. An individual could complain about this interprovincial transaction to our Office. Alternatively, an individual who wants to complain about the disclosure of personal information by the Alberta company could direct the complaint to the Alberta Information and Privacy Commissioner under Alberta's *PIPA*. However, if the individual is complaining about the collection in Saskatchewan of their personal information, he or she may direct the complaint to the Privacy Commissioner of Canada, as Saskatchewan does not have substantially similar legislation in place governing its private sector organizations' activities. Whether the complaint is initiated in Alberta, with our Office, or both, our respective offices will work together to coordinate our work where possible.

Sometimes the jurisdictional issue is entangled. In one case handled by our Office, the complainant worked for an organization in one of the western provinces that has substantially similar legislation. The organization provides disability insurance. The individual applied to the insurance company, located in Quebec, for access to her files. Those files are kept in Toronto. The insurance company responded as if *PIPEDA* regulated the question. Is *PIPEDA* the appropriate legislation or does it fall to one of the provinces?

In another case, an individual worked for a company in one of the western provinces with substantially similar legislation. Through the company, the individual had an employee assistance program (EAP) in Ontario, and complained about a disclosure by the EAP. Because Ontario does not yet have substantially similar legislation, *PIPEDA* would apply in Ontario. But is this an Ontario issue – because the EAP is located in Ontario – or is it within the jurisdiction of the western province under that province's private sector legislation?

**Streamlining our approach to jurisdictional issues**

Federal and provincial Commissioners are working together to resolve jurisdictional challenges. This process has been collegial, not confrontational. Some individuals may raise jurisdictional matters in the courts but these issues can largely be resolved through discussion. Our goal in every case is to establish as simple and clear a mechanism as possible for individuals and organizations.

One way we have sought to streamline our approach to jurisdictional and related investigative issues is to establish a regional private sector privacy forum with Alberta

and British Columbia. This forum operates under the authority of the federal and provincial Commissioners and seeks to coordinate and harmonize federal and provincial oversight of the private sector in Canada. Senior investigations and legal staff from each of the Commissioners' offices take part in monthly teleconferences and twice-yearly meetings. The forum serves many functions, but among the most important is to develop procedures for determining jurisdiction, transferring complaints and conducting parallel investigations.

Federal and provincial Commissioners have also been working to develop protocols for handling investigations where there may be overlapping jurisdiction. In March 2004, the Privacy Commissioner of Canada sent a letter of understanding to the Information and Privacy Commissioners of Alberta, British Columbia, and a similar letter to the Ontario Information and Privacy Commissioner in January 2005, to confirm discussions about the handling of complaints relating to organizations in those provinces. In part, these letters of understanding set out how our Office would handle complaints both before and after a finding of "substantially similar" occurs in respect of the provincial laws.

These letters of understanding are available on the Privacy Commissioner of Canada's Web site ([www.privcom.gc.ca](http://www.privcom.gc.ca)). There is further information about jurisdictional issues, including a fact sheet, on our Web site, as well as on the Web sites of other provincial Information and Privacy Commissioners.

Our Office has had a long-standing relationship with the *Commission d'accès à l'information* (CAI) in Quebec. Quebec was the first Canadian jurisdiction to adopt private sector privacy legislation in 1994. In order to take advantage of the rich body of jurisprudence accumulated in Quebec since 1994, we have commissioned a document to review and summarize Quebec's experience to date.

In order to ensure that this may be as helpful as possible to all jurisdictions, we established an External Editorial Board to assist in the project. The members are:

Madeleine Aubé, General Counsel, Commission d'accès à l'information du Québec

Jeffrey Kaufman, Fasken Martineau, Toronto

Mary O'Donoghue, Senior Counsel, Ontario Information and Privacy Commissioner's Office

Murray Rankin, Arvay Finlay, Victoria

Frank Work, Q.C., Information and Privacy Commissioner of Alberta

This document was published in August 2005 and is available on our Web site.

The Alberta and federal Commissioners have already cooperated in investigating issues that have both federal and provincial elements – see for example, the case summary relating to a joint federal/provincial investigation of misdirected medical information mentioned below in the section on Incidents under *PIPEDA*. In another case, Edmonton police conducting an investigation found information used in determining security clearances for Alberta government employees. The information included credit reports. The aspects of the investigation relating to correction of erroneous credit reports fell to the Alberta Information and Privacy Commissioner, while our Office handled the systemic issue of retention of credit reports.

While the constitutional pitfalls may be numerous, we hope a practical approach to the application of the way personal information protection legislation in Canada will yield, overall, effective privacy protection in Canada.





# Evolution of the *Personal Information Protection and Electronic Documents Act*

## Statutory Changes

### *PIPEDA* Amendments

The *Public Safety Act, 2002*<sup>1</sup> included two amendments to *PIPEDA*. Their effect is to permit organizations to collect and use personal information without consent for the purposes of disclosing this information when required by law or to government institutions if the information relates to national security, the defence of Canada or the conduct of international affairs.

The Commissioner appeared before the Senate Standing Committee on Transport and Communications on March 18, 2004, to voice her concerns about these amendments.<sup>2</sup> In her statement to the Committee, the Commissioner pointed out that the amendments will allow organizations to act as agents of the state by collecting information without consent for the sole purpose of disclosing it to government and law enforcement agencies. She asked that the changes to *PIPEDA* be dropped, and expressed concern that the wording of these changes was so broad that they could apply to any organization subject to *PIPEDA*, with no limit on the amount of information to be collected or the sources of the information.

The *Public Safety Act, 2002*, without the changes recommended by the Commissioner, came into force on May 11, 2004.

---

<sup>1</sup> See [http://www.parl.gc.ca/PDF/37/3/parlbus/chambus/house/bills/government/C-7\\_4.pdf](http://www.parl.gc.ca/PDF/37/3/parlbus/chambus/house/bills/government/C-7_4.pdf)

<sup>2</sup> See [http://www.privcom.gc.ca/speech/2004/sp-d\\_040318\\_e.asp](http://www.privcom.gc.ca/speech/2004/sp-d_040318_e.asp)

## Amendments to Other Acts

The *Federal Court Rules, 1998* were enacted before *PIPEDA*. Because of this, rule 304(1)(c), which deals with service of a “notice of application”, had no reference to *PIPEDA*. Accordingly, in February 2003 our Office’s Legal Branch requested an amendment to rule 304(1)(c) to include notifying the Privacy Commissioner whenever an application is filed under *PIPEDA*, as well as when one is filed under the *Privacy Act*.

The *Rules Amending the Federal Court Rules, 1998* came into force on November 29, 2004 and were published in the *Canada Gazette, Part II* of December 15, 2004 as SOR/2004-283. Section 16 of this document amended rule 304(1)(c) to include *PIPEDA* so that the text of that section now reads:

[...] 304(1)(c) where the application is made under the *Access to Information Act*, Part 1 of the *Personal Information Protection and Electronic Documents Act*, the *Privacy Act* or the *Official Languages Act*, the Commissioner named for the purposes of that Act; and [...]

## 2006 Review of *PIPEDA* by Parliament

The Office has been preparing for the upcoming review of *PIPEDA* by Parliament, scheduled to take place in 2006. The year 2006 may appear a long way off from the vantage point of this 2004 Annual Report, but our experience over the past four years in overseeing the application of the law has convinced us that this a good time to begin preparing, and that our Office is also the right place to begin. This Office will be active in developing policy positions to make the operation of the law simpler and more effective for organizations and individuals alike, and to ensure that the fair information practices at the heart of *PIPEDA* are translated into practice.

Like any significant new law, *PIPEDA* has its problems. It is hard to get the first version of any law completely “right”, particularly when it is breaking new ground and providing new rights and obligations. We don’t have all the solutions for these problems, but we have identified several issues and, in some cases, suggested possible ways to address them.

- **Scope**

- Does *PIPEDA* deal effectively with employee information? Many of our complaints arise in the context of the employer/employee relationship. The current *PIPEDA* doesn't always fit that relationship. Both the B.C. and Alberta private sector legislation deal with employee information under a separate set of rules.
- There are clear overlaps between *PIPEDA* and the *Canada Labour Code* and between the mandate of the Office of the Privacy Commissioner and that of labour arbitrators.
- There remains uncertainty about the distinction, if there is one, between "commercial" activity, as defined in the Act, and "professional" services.
- Elsewhere in this report, we describe a case that involved sending unsolicited commercial e-mail to a business e-mail address. The legislated definition of "personal information" excludes certain business information such as address and phone number. Should business e-mail addresses also be excluded?

- **Consent**

- Consent is at the heart of *PIPEDA*. It is also one of the most problematic issues under the Act. For example, must an organization obtain the consent of all its customers when it proposes to disclose their information in the context of a business merger or acquisition? That seems to be what the law requires, but it is not always practicable for several sound business reasons. The B.C. and Alberta private sector laws both deal with this issue head-on and establish rules to protect customer information in these circumstances. Should *PIPEDA* do the same?

- **Oversight**

- *PIPEDA* gives the Commissioner the powers of an ombudsman – in other words, no power to issue an order or levy a penalty against an organization violating *PIPEDA*. While we think that the ombudsman model works well overall (in fact, even in jurisdictions that have order-making powers on privacy matters, the vast majority of cases are settled without an



order) we are aware that oversight bodies in other jurisdictions have enforcement powers. Parliament may want to consider the advantages and disadvantages of both models in its 2006 review of *PIPEDA*.

These are simply a few of the issues that may need to be addressed in the five year review of the Act.

# Complaints

In 2004, *PIPEDA* reached its full extension, to cover all commercial activities in provinces without substantially similar legislation. Over the year, we saw a significant spike in complaints filed under *PIPEDA*: we received 723 complaints between January 1 and December 31, more than double the 302 received in the previous calendar year. The expansion of the Act's coverage appears to be a considerable factor in the increase. Financial institutions were once again the most frequent object of complaints, as one might expect given the vast quantities of personal information that pass through their hands. They were followed by the telecommunications sector, also a front-runner in years past. But complaints in four areas new to us – insurance, sales, accommodation, and professionals – accounted between them for over 25 per cent of the complaints. It remains to be seen whether we will see further increases, as the Act becomes better known to Canadians.

## PIPEDA COMPLAINTS RECEIVED BETWEEN JANUARY 1 AND DECEMBER 31, 2004

### Sectoral Breakdown

Sector	Count	Percentage
Financial Institutions	212	29.3%
Telecommunications	125	17.3%
Insurance	82	11.3%
Sales	82	11.3%
Transportation	67	9.3%
Health	36	5%
Accommodation	18	2.5%
Professionals	15	2.1%
Services	10	1.4%
Other	76	10.5%
<b>Total</b>	<b>723</b>	<b>100%</b>

The complaints related to the following concerns:

**Breakdown by Complaint Type**

<b>Complaint type</b>	<b>Count</b>	<b>Percentage</b>
Use and Disclosure	286	39.6%
Collection	172	23.8%
Access	112	15.5%
Safeguards	40	5.5%
Consent	37	5.1%
Accuracy	22	3%
Correction/Notation	11	1.5%
Fee	12	1.7%
Other	4	0.6%
Retention	6	0.8%
Accountability	9	1.2%
Time Limits	9	1.2%
Challenging Compliance	1	0.2%
Openness	2	0.3%
<b>Total</b>	<b>723</b>	<b>100%</b>

During the year, we closed 379 complaints. This is an improvement over the previous year, where we closed 278. Nonetheless, in both years we received more complaints than we closed. This presents the Office with the risk of a developing backlog.

We are taking initiatives to address this, including reallocating resources and reviewing the way in which we conduct our investigations. One of the most promising approaches may be a new emphasis, since January 2004, on a category of complaint disposition, “Settled during the course of the investigation.” These are cases in which, during the investigation, we have helped bring about a solution satisfactory to all parties.

**COMPLAINT INVESTIGATIONS TREATMENT TIMES – PIPEDA**

This table represents the average number of months it has taken to complete a complaint investigation by disposition, from the date the complaint is received to when a finding is made.

**By Disposition**

For the period between January 1 and December 31, 2004.

<b>Disposition</b>	<b>Average Treatment Time in Months</b>
Early resolution	2.9
Discontinued	5.6
Settled	7.2
No jurisdiction	7.8
Overall average	8.3
Resolved	10.5
Not well-founded	11.0
Well-founded	11.0
Overall Average	8.3

**By Complaint Type**

For the period between January 1 and December 31, 2004.

<b>Complaint Type</b>	<b>Average Treatment Time in Months</b>
Fee	3.4
Accuracy	6.4
Consent	6.9
Time Limits	8.1
Use and Disclosure	8.2
Access	8.3
Safeguards	8.4
Correction/Notation	8.5
Collection	8.9
Retention	9.5
Accountability	12.0*
Challenging compliance	12.0*
Overall average	8.3

\* The average treatment times for these two complaint types in fact represent one case for each.

Settling complaints in investigation is not new, but our emphasis on it is. In 2003, settled cases represented two per cent of our completed cases. In contrast, of the 379 cases concluded in 2004, 152 – just over 40 per cent – fell in the “settled” category. This was by far the most frequent disposition of our cases.

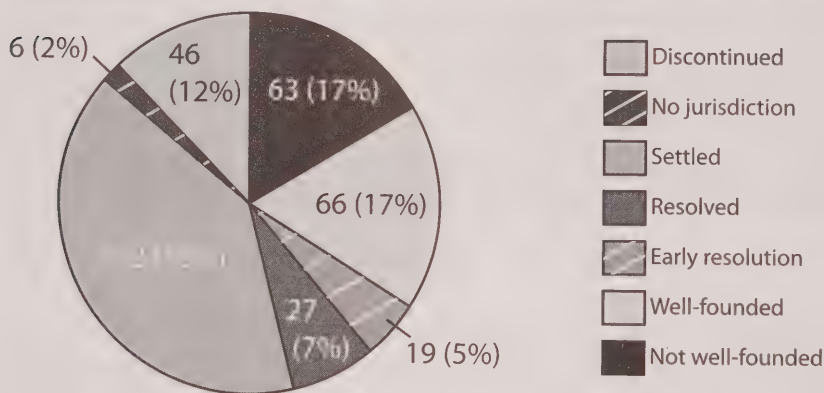


This new emphasis on settlement is an important element in dealing with the volume of complaints that we face. Over the course of the year, settlement of a complaint took, on average, less time than any other complaint resolution except discontinuance (where, for instance, the complainant may no longer want to pursue the matter or cannot be located) or early resolution, where the issue is dealt with before any investigation takes place.

If we take the figures for the “settled” and “early resolution” categories, we can see that 45 per cent of our complaints are concluded without the investment of resources entailed in a complete investigation. This is welcome news to an organization facing an increasing workload.

That we were able to settle so many of our cases suggests that organizations and individual complainants welcome the opportunity to resolve complaints expeditiously and pragmatically. This fits well with our ombudsman role; we are in this business, after all, to help people resolve problems. At the same time, of course, we have a responsibility to ensure that the public policy intentions of *PIPEDA* are respected. Our Office, as much as the complainant and the organization, has an interest in any settlement; our view, however, is that enthusiasm for settlement does not mean settling complaints at any cost. Our investigators work closely with the parties in the settlement process to ensure that systemic issues raised in a complaint are addressed.

#### COMPLAINTS CLOSED BETWEEN JANUARY 1 AND DECEMBER 31, 2004: TYPE OF CONCLUSION

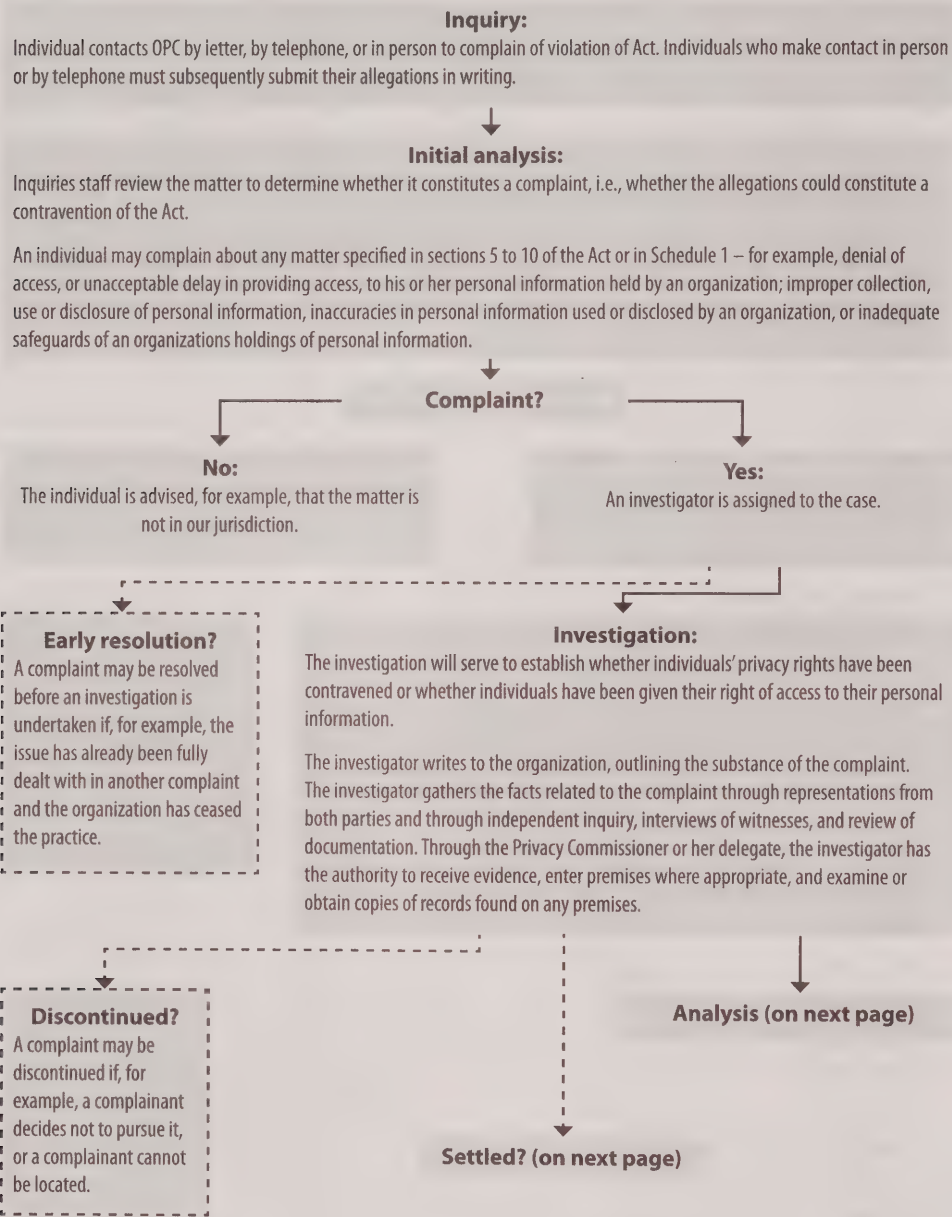


**Definitions of Complaint Types under PIPEDA**

Complaints received in the Office are categorized according to the principles and provisions of *PIPEDA* that are alleged to have been contravened:

- **Access.** An individual has been denied access to his or her personal information by an organization, or has not received all his or her personal information, either because some documents or information are missing or the organization has applied exemptions to withhold information.
- **Accountability.** An organization has failed to exercise responsibility for personal information in its possession or custody, or failed to identify an individual responsible for overseeing its compliance with the Act.
- **Accuracy.** An organization has failed to ensure that the personal information that it uses is accurate, complete, and up-to-date.
- **Challenging compliance.** An organization has failed to put procedures or policies in place that allow an individual to challenge its compliance with the Act, or has failed to follow its own procedures and policies.
- **Collection.** An organization has collected personal information that is not necessary, or has collected it by unfair or unlawful means.
- **Consent.** An organization has collected, used, or disclosed personal information without valid consent, or has made the provision of a good or service conditional on individuals consenting to an unreasonable collection, use, or disclosure.
- **Correction/Notation.** The organization has failed to correct personal information as requested by an individual, or, where it disagrees with the requested correction, has not placed a notation on the information indicating the substance of the disagreement.
- **Fee.** An organization has required more than a minimal fee for providing individuals with access to their personal information.
- **Retention.** Personal information is retained longer than necessary for the fulfillment of the purposes that an organization stated when it collected the information, or, if it has been used to make a decision about an individual, has not been retained long enough to allow the individual access to the information.
- **Safeguards.** An organization has failed to protect personal information with appropriate security safeguards.
- **Time Limits.** An organization has failed to provide an individual with access to his or her personal information within the time limits set out in the Act.
- **Use and Disclosure.** Personal information is used or disclosed for purposes other than those for which it was collected, without the consent of the individual, and the use or disclosure without consent is not one of the permitted exceptions in the Act.

# Investigation Process under *PIPEDA*



**Analysis:**

The investigator analyses the facts and prepares recommendations to the Privacy Commissioner or her delegate. The investigator will contact the parties and review the facts gathered during the course of the investigation. The investigator will also tell the parties what he or she will be recommending, based on the facts, to the Privacy Commissioner or her delegate. At this point, the parties may make further representations.

Analysis will include internal consultations with, for example, Legal Services or Research and Policy Branches, as appropriate.

**Settled?**

The OPC seeks to resolve complaints and to prevent contraventions from recurring. The Commissioner encourages resolution through mediation, negotiation and persuasion. The investigator assists in this process.

**Findings:**

The Privacy Commissioner or her delegate reviews the file and assesses the report. The Privacy Commissioner or her delegate, not the investigator, decides what the appropriate outcome should be and whether recommendations to the organization are warranted.

The Privacy Commissioner or her delegate sends letters of findings to the parties. The letters outline the basis of the complaint, the relevant findings of fact, the analysis, and any recommendations to the organization. The Privacy Commissioner or her delegate may ask the organization to respond in writing, within a particular timeframe, outlining its plans for implementing any recommendations.

The possible findings are:

**Not Well-Founded:** The evidence, on balance, does not lead the Privacy Commissioner or her delegate to conclude that the complainant's rights under the Act have been contravened.

**Well-Founded:** The organization failed to respect a provision of the Act.

**Resolved:** The evidence gathered in investigation supports the allegations raised in the complaint, but the organization agreed to take corrective measures to rectify the problem, to the satisfaction of this Office.

In the letter of findings, the Privacy Commissioner or her delegate informs the complainant of his or her rights of recourse to the Federal Court.

Where recommendations have been made to an organization, OPC staff will follow up to verify that they have been implemented.

The complainant or the Privacy Commissioner may choose to apply to the Federal Court for a hearing of the matter. The Federal Court has the power to order the organization to correct its practices, to publish a notice of any action taken or proposed to correct its practices. The Court can award damages to a complainant, including damages for humiliation. There is no ceiling on the amount of damages.

**Note:** a broken line (---) indicates a *possible* outcome.



## Definitions of Findings under *PIPEDA*

The Office has developed a series of definitions of “findings” to explain the outcome of its investigations under *PIPEDA*:

**Not well-founded:** This means that the investigation uncovered no or insufficient evidence to conclude that an organization violated the complainant’s rights under *PIPEDA*.

**Well-founded:** This means that an organization failed to respect a provision of *PIPEDA*.

**Resolved:** This means that the investigation substantiates the allegations, but that the organization has taken or has committed to take corrective action to remedy the situation, to the satisfaction of our Office.

**Settled during the course of the investigation:** This means that the Office has helped negotiate a solution that satisfies all involved parties during the course of the investigation. No finding is issued.

**Discontinued:** This means that the investigation ended before a full investigation of all the allegations. A case may be discontinued for any number of reasons — for instance, the complainant may no longer want to pursue the matter or cannot be located to provide information critical to making a finding.

**No jurisdiction:** This means that the investigation leads to a conclusion that *PIPEDA* does not apply to the organization or to the activity that is the subject of the complaint.

**Early resolution:** This is a new type of disposition. It applies to situations where the issue is dealt with before a formal investigation occurs. For example, if an individual files a complaint about a type of issue that the Office has already investigated and found to comply with *PIPEDA*, we would explain this to the individual. “Early resolution” would also apply when an organization, on learning of allegations against it, addresses them immediately to the satisfaction of the complainant and this Office.

**FINDINGS BY COMPLAINT TYPE**

Complaints closed between January 1 and December 31, 2004

	Discontinued	Early Resolution	No Jurisdiction	Not Well- founded	Resolved	Settled	Well- founded	TOTAL
Access	10	3	2	8	5	20	14	62 (16%)
Accountability	0	0	0	0	0	1	0	1 (0%)
Accuracy	2	1	0	1	0	1	0	5 (1%)
Challenging Compliance	0	0	0	0	0	0	1	1 (0%)
Collection	10	2	1	25	15	30	13	96 (25%)
Consent	2	1	0	0	0	3	1	7 (2%)
Correction/ Notation	0	0	0	0	0	1	1	2 (1%)
Fee	0	2	1	0	0	2	0	5 (1%)
Retention	0	0	0	0	1	1	0	2 (1%)
Safeguards	0	0	1	2	0	13	2	18 (5%)
Time Limits	0	0	0	2	1	3	1	7 (2%)
Use and Disclosure	22	10	1	25	5	77	33	173 (46%)
<b>TOTAL</b>	<b>46</b>	<b>19</b>	<b>6</b>	<b>63</b>	<b>27</b>	<b>152</b>	<b>66</b>	<b>379</b>
<b>(# and %)</b>	<b>(12%)</b>	<b>(5%)</b>	<b>(2%)</b>	<b>(17%)</b>	<b>(7%)</b>	<b>(40%)</b>	<b>(17%)</b>	

## Inquiries

The Inquiries Unit responds to requests for information from the public about the application of *PIPEDA* as well as the *Privacy Act*. The Office receives thousands of inquiries each year from the public and organizations seeking advice on private sector privacy issues.

In 2004, the Office received 12,132 *PIPEDA* inquiries, down from 2003, when we received 13,422. The decline may be attributable to greater understanding of *PIPEDA* among the organizations that are subject to it; in 2003, many organizations were searching for guidance as they anticipated the full implementation of *PIPEDA* on January 1, 2004.

In the course of the year, staff shortages in the Inquiries Unit coupled with the ongoing heavy volume of work have presented challenges. As a result, it was necessary

to reassess the way we respond to public inquiries. We no longer accept or respond to inquiries or complaints by e-mail. We introduced an automated telephone system to answer the public's most frequently asked questions such as those about identity theft, telemarketing and, of course, the social insurance number. And we continue adding information to our Web site to answer the most frequently asked questions. We also temporarily assigned some investigators to help the unit. Lastly, we now invite individuals to telephone during office hours since we can often determine a caller's needs faster and better in person than in a series of e-mails and letters.

### **INQUIRIES STATISTICS**

January 1 to December 31, 2004

The following table represents the total number of *PIPEDA* inquiries responded by the Inquiries Unit.

Telephone inquiries	8,861
Written inquiries (letter, email or fax)	3,271
Total number of inquiries received	12,132

### **Inquiries Response Times**

On average, written inquiries (one quarter of the workload of the Unit) were responded to within three months. Nearly 3/4 of our inquiries were received by telephone. The majority of these were responded to immediately; the remainder, which may have required research, were responded to within one to two weeks.

Providing written responses to inquiries is very time consuming and labour intensive. Over the year, the Inquiries Unit accrued a backlog of inquiries which exacerbated the average monthly response times. As we implement new measures, we will monitor the situation to determine whether these changes have resulted in efficiency gains.

## Select Cases under PIPEDA

The following cases illustrate the breadth and variety of the cases investigated by our Office. We also posted 29 summaries of findings for 2004 on our Web site.

### **Medical information divulged through indiscreet choice of words**

Even with the best of intentions, and even in such seemingly harmless activities as arranging for a taxi, health professionals must watch what they say to company managers about employees' health situations.

#### ***The facts***

After completing a substance abuse program, a complainant signed a "last chance" contract as a condition of continued employment with a national transportation company. This contract required him to submit to regular monitoring, as well as random drug and alcohol testing, by the company's health service provider. The complainant was very concerned about confidentiality and for the most part had managed to keep his situation from fellow employees and supervisors.

One day while he was at home on active furlough, he received a call from a nurse, who told him he had to be at the clinic within four hours to give a urine sample. When he told the nurse he had no way of getting there, she said she would call the company and arrange for a taxi. The complainant soon got a call from his supervisor, who told him a taxi would take him "to the lab". The supervisor then asked him whether he was "under contract" – meaning a last-chance contract.

From the supervisor's words, the complainant assumed that the nurse had revealed too much information about him. Angered by what he believed to be a breach of his confidentiality, he later confronted both the nurse and the supervisor in abusive language that the company deemed to be grounds for disciplinary action. An investigation ensued, and the complainant was eventually dismissed for conduct unbecoming an employee (he has since been reinstated).

The supervisor told our Office that he had assumed the complainant's involvement in the substance abuse monitoring program from the nurse's use of the words "test" and "clinic" in his telephone conversation with her. The nurse, on the other hand, told us that she had used the word "appointment", not "test". She claimed to have given the supervisor only the minimum information necessary to make it clear that a taxi was needed and that there was a reasonable basis for the company to pay for it.



At one point, the company's regional superintendent had asked the nurse to document her version of the events relating to the complainant's alleged misconduct. She did so in an e-mail, which was sent to the regional superintendent and later forwarded to two other senior managers. In the e-mail, the nurse stated that the complainant had been required to undergo a "medical test ... to assure his continuing fitness for duty" and that he had had to take the test within four hours after her phone call to him. Believing that this information implied his participation in the program, the complainant objected that it had been conveyed to the parties in question.

The complainant's allegation to our Office was that the nurse had inappropriately divulged his personal information to his supervisor in a telephone conversation and to other senior managers in an e-mail message.

### ***Our findings***

With respect to the telephone conversation, though it seemed appropriate that the nurse would have had to provide the supervisor with a reason to justify the taxi request, our investigation could not establish what exactly she had said to the supervisor. Whatever wording she used, it either caused the supervisor to conclude, or confirmed his suspicion, that the complainant was in the substance abuse monitoring program.

Similarly with respect to the e-mail, we did not dispute the need to inform senior managers of the complainant's alleged misconduct, but the problem was the information's content. Since the nurse's purpose had been to document the complainant's behaviour, stating that he had been required to go for a medical test within four hours was superfluous. The words "medical appointment" would have been sufficient to explain the need for a taxi.

The company was therefore found to have inappropriately used the complainant's personal information in contravention of Principle 4.3 of the Act. The complaint was well-founded.

### **Professor objects to getting spammed at the office**

Is a person's business e-mail address fair game for marketers?

### ***The facts***

At his university office, a complainant received an unsolicited commercial e-mail promoting season's tickets for a professional team's games. The sales agent in question admitted to having obtained the e-mail address from the university's Web site, and he

agreed not to send the complainant further e-mails without his consent. Two weeks later, however, the complainant received a second e-mail solicitation from the same organization, but a different sales agent.

The complainant's allegation to our Office was that the organization had collected and used his personal information without his consent.

The organization did not dispute that it had sent the complainant a solicitation at his office e-mail address on two occasions. The two sales representatives in question were each responsible for a different solicitation "program" – one the "university program", and the other the "lawyer program". The agent responsible for the lawyer program had generated his contact list from the Web site of a law firm with which the complainant was associated. There was no cross-referencing system in place to flag the complainant's previous request that his name be deleted from the organization's marketing lists.

In response to the complaint, the organization removed the complainant's name from all its marketing lists and instituted cross-selling controls to ensure similar treatment of any future objection. The organization has also engaged a new ticketing and sales firm that is more knowledgeable about the requirements of *PIPEDA*.

The view of the university in question is that the e-mail addresses of its staff are business information. The university generally requires its faculty members to agree to have their business e-mail addresses published, in accordance with its business model and its expectation that employees be easily accessible. However, the university also expects a business or organization to obtain permission before contacting faculty for purposes unrelated to promoting the university's interests.

Section 2 of the Act specifically excludes the name, title, or business address or phone number of an employee of an organization from the definition of personal information, but makes no mention of an employee's business e-mail address. Sections 7(1)(d) and 7(2)(c.1) stipulate that an organization may collect and use personal information without the individual's knowledge and consent if the information is publicly available and specified in the regulations.

The regulations applying to these sections state that publicly available information includes an individual's name, title, address, and telephone number appearing in a professional or business directory, listing, or notice that is available to the public, where the collection, use, and disclosure of the personal information relate directly to the purpose for which the information appears.

### ***Our findings***

We determined first that, since section 2 does not specify a business e-mail address as being among the excluded types of information, it must therefore be deemed personal information for purposes of the Act.

The question then to be considered was whether the sports organization could rely on the exceptions to consent set out in sections 7(1)(d) and 7(2)(c.1).

The university had listed faculty e-mail addresses on its Web site with the expectation that businesses, organizations, and individuals might contact faculty members to further the university's interests. The sale of season's tickets to a sporting event, however, was not related to that purpose. The same reasoning applied to the Web site of the firm with which the complainant was associated. Moreover, even after the complainant's initial objection, the organization had collected his e-mail address from that other source and used it again for marketing purposes against his explicit instructions.

In sum, we determined that, since the purposes for which the organization had collected and used the complainant's personal information was entirely unrelated to the reason for which the information had been published, the organization could not rely on the exceptions to consent. The organization had thus collected and used the complainant's personal information without his consent, in contravention of Principle 4.3 of the Act. The complaint was well-founded.

### **Video surveillance as a last resort**

Our Office considers video surveillance an extremely privacy-invasive form of technology. The medium's very nature entails the collection of a great deal of personal information, much of which may relate to innocent third parties, may be extraneous, or may lead to judgments about the subject that have nothing to do with the original purpose for collecting the information.

Only as a last resort should companies use video surveillance for investigative purposes – especially in investigating employees away from the workplace.

### ***The facts***

Over the course of his employment with a company, a complainant had reported a number of work-related injuries and had eventually requested workplace accommodation for physical limitations. For almost two years, the company attempted to satisfy his accommodation requests, but to no avail. The complainant

grew increasingly dissatisfied with the company's efforts, unwilling to perform his work duties, and resistant to the company's repeated requests for up-to-date medical information.

In view of the complainant's behaviour and lack of cooperation in providing accurate information about his ability to perform certain job-related tasks, the company became increasingly suspicious about the extent of his physical limitations. It eventually requested that he undergo an independent medical assessment, which he initially refused but in the end accepted. The independent assessors concluded that, although the complainant did have physical limitations, there also appeared to be many "non-physical barriers" to his returning to work. The assessors also noted that further functional testing would be unlikely to provide an accurate assessment of the complainant's true functional abilities.

Two months later, while the complainant was on leave, the company hired a private investigator to conduct surveillance on him with a view to determining whether he was being truthful about his physical limitations. After two weeks, the investigator provided the company with a report and eight hours of videotape showing the complainant performing tasks of which he had claimed to be incapable. On this evidence that he had misrepresented the state of his health, the company dismissed him.

The complainant's allegation to our Office was that his employer had collected his personal information by way of video surveillance without his knowledge and consent and had used that information to terminate his employment.

To justify its actions in this case, the company relied on sections 7(1)(b) and 7(2)(d) of the Act. These provisions permit an organization to collect and use personal information without the individual's knowledge and consent if seeking knowledge and consent would compromise the availability or the accuracy of the information and if the collection and use are reasonable for purposes of investigating a breach of an agreement or a contravention of a law.

The company maintained that its decision to conduct video surveillance was the result of consultation among a small team of legal, medical, and industrial-relations professionals, who had determined that such a measure was necessary as a last resort in the circumstances. The company had provided information about the complainant's physical limitations and had instructed the investigator to monitor the complainant's activities over a significant-enough period to provide a complete picture of his capability and establish sound, factual, and irrefutable evidence of his fraudulent behaviour. The



company acknowledged, however, that it had no formal policy or procedures in place to guide managers in such situations.

### ***Our findings***

There was no question that the company had collected the complainant's personal information through video surveillance without his knowledge and consent. The issue was whether section 7(1)(b) could apply. However, this exception could not be read in isolation. Among the factors to consider were whether the organization had substantial evidence to support the suspicion that the relationship of trust had been broken, could show that it had exhausted all other means of obtaining the information that it required in less privacy-invasive ways, and had limited the collection to the purposes as far as possible.

On the evidence, our Office was satisfied that the company's purpose of determining whether the complainant was violating his employment contract by misrepresenting the state of his health was based on substantial evidence. Furthermore, the company had made numerous less privacy-invasive attempts to gather the information it had required, but these had mostly met with resistance from the complainant and in the end had not dispelled the organization's concerns. It had also, in taking the step of hiring the private investigator, outlined what information it was seeking and focused the collection of personal information as far as possible.

In sum, the company had had reasonable cause to believe that the complainant was violating his employment contract, and had clearly had difficulty in obtaining accurate information from him with his knowledge and consent. We accepted the company's reliance on sections 7(1)(b) and 7(2)(d) to collect and use the complainant's personal information without his knowledge and consent. The complaint was not well-founded.

Notwithstanding the findings, we recommended that the company formalize the measures it had taken by developing privacy-conscious policy and practices regarding the use of video surveillance. Such policy should consider the following:

- Video surveillance is a last resort and should only be contemplated if all other avenues of collecting personal information have been exhausted.
- The decision to undertake video surveillance should occur at a very senior level of the organization.

- The private investigator should be instructed to collect personal information in accordance with the Act, and should be especially mindful of Principle 4.4 (Limiting Collection).

The company implemented this recommendation.

### **Cameras in the workplace: The importance of stating purposes**

Employees naturally tend to resent the presence of video cameras on the job. However, by being forthcoming about purposes, the employer can often alleviate employees' fears about loss of privacy.

#### ***The facts***

Implementing a recommendation from a security review, a broadcasting company installed three surveillance cameras at its workplace – one outside and two inside the building. The outside camera captured the parking lot and building entrance, and the inside cameras aimed at the interior entrance and a central corridor.

Several employees of the company lodged complaints with our Office, alleging that the company was using the cameras to collect their personal information, particularly about their behaviour and work performance.

The employer maintained that a memorandum had been posted to inform employees of the camera installation and its true purpose, which was to ensure the safety and well-being of employees by tracking non-employee traffic in and out of the building. The employees, however, were not aware of the memorandum.

During our investigation, the company agreed to inform employees of the purposes for which information collected by the cameras would be used. It also agreed to develop a policy document on the use of surveillance cameras, including the objectives, installation sites, employees authorized to operate the system, time of surveillance and recording, and applicable equity principles.

The company subsequently fulfilled these commitments.

#### ***Our findings***

The company had not made reasonable efforts to inform its employees and had thereby violated Principle 4.3.2 of the Act.

However, it was also established that the use of such a surveillance system constituted an appropriate means of protecting employees. Since the cameras were not to be used to collect employees' personal information and were not installed in places where there was a reasonable possibility of privacy invasion, it did not seem appropriate that the employer be required to obtain employees' consent for their use. If the cameras inadvertently collected employees' personal information, the employer would not be able to use such information without the employees' consent except in the circumstances set out in the sections 7(2)(a) and (b) of the Act (these provisions apply to legal investigations and emergencies, respectively).

Because of the company's commitments to inform employees and develop a policy document, the complaints were deemed resolved.

### **Cameras in the workplace: The importance of keeping to reasonable purposes**

In this case, our Office supported the use of video cameras to enhance the safety of the workplace, but warned that the unrestrained use of such cameras to monitor employee productivity or to manage the employer/employee relationship would have a chilling effect on employee morale. Employers using cameras for legitimate operational purposes must make every effort to keep to those purposes, and must exercise great care and deliberation in resorting to video surveillance for any exceptional purposes allowable under the Act.

#### ***The facts***

A railway company uses cameras to monitor train movements and to inform crew members of train locations. The company installed the cameras after a risk analysis, and both the company and the employee union agree that the cameras are needed for operational purposes.

One day the manager responsible for the cameras spotted two on-duty employees getting into a car. He went into his office and used the cameras' zoom capacity to determine that the employees were driving off site. The company subsequently imposed a disciplinary penalty against them for leaving work without permission. One of the two employees grieved the discipline, and the matter was referred to arbitration. Both employees complained to our Office that the company had used video cameras, ordinarily used for operational purposes, to determine that they were leaving company property during regular working hours.

The company argued initially that the Commissioner should exercise her discretion not to issue a report of findings, since the matter was also being dealt with through arbitration. Referring to a recent decision of the Federal Court to the effect that labour tribunals have exclusive jurisdiction over disputes arising out of collective agreements, the company later contended that the Commissioner's Office did not have jurisdiction with respect to such complaints.

The company also argued that the Act allows organizations to collect, use, and disclose information for purposes that a reasonable person would consider appropriate in the circumstances. It denied actually having *collected* the complainants' personal information, since the camera did not record. It described the camera as a "visual aid" that had allowed the manager to follow up on a concern he had already identified without the use of a camera. It maintained that the complainants had had no reasonable expectation of privacy, given that the rail yard was constantly busy with pedestrian traffic. It contended that, given the complainants' suspicious behaviour on the day in question, a reasonable person would have considered it appropriate to use the cameras as a visual aid to determine the direction of their vehicle.

Finally, the company referred to section 7(1)(b) and argued that, should the Commissioner conclude that the camera had indeed collected the complainants' personal information, their consent to the collection and use of the information had not been required since the company was investigating a breach of an employment condition at the time.

### ***Our findings***

The Office observed first that the Federal Court decision to which the company had referred was under appeal. We therefore concluded that we had jurisdiction to investigate the complaints.

The Office also declined to exercise its discretion not to deal with the complaints. We referred to the lead role of the Office in determining whether organizations are adhering to the *Act* and in educating both organizations and the public about the Act. We noted that the complaints raised issues that could set a precedent.

We concluded as follows:

- The *Act* does not restrict the definition of personal information to information that is recorded only, but rather clearly defines personal information as including any information about an identifiable individual. The cameras in question do



collect the personal information of employees, and were used to collect the complainants' personal information – that is, the fact that they were leaving the yard during work hours.

- There is no question that the customary use of the cameras to enhance the safety of the workplace is appropriate in the circumstances, as contemplated by section 5(3) of the Act. The cameras were installed after a risk analysis, and both union and management support their use.
- Regarding the appropriateness of using the cameras in the circumstances surrounding the complaints, the company did not present any evidence that unauthorized absences from the workplace were a persistent problem with the complainants or with other employees. The company did not present any evidence of other, less intrusive efforts it had taken to manage unauthorized absences. A reasonable person would not consider it appropriate to use the cameras to manage a workplace performance issue. In the circumstances, the use was contrary to section 5(3) of the Act.
- Where an employer suspects that the relationship of trust has been broken, it can initiate the collection of information to investigate that breach without the consent of the individual. However, the only evidence the company presented to suggest a possible breach in the relationship of trust was that the employees in question had been seen entering a private vehicle. The company admitted that the employees might have been leaving the site with the permission of their immediate supervisor and that the manager who used the camera had only determined *after the fact* that the employees left the work site without permission. Cameras being highly privacy-intrusive, a decision to use them, even in the circumstances set out in section 7(1)(b), must be taken with great care and deliberation. Where there is a less intrusive method of achieving the same result, that method should be the first choice.

We concluded that the complaints were well-founded.

**Bank customers required to declare citizenship**

This complaint, specifically about a bank's collection and use of personal information, also raised a general concern about whether a bank was putting the requirements of foreign legislation ahead of the privacy interests of its Canadian customers.

***The facts***

Several account holders complained when their bank sent them a form letter asking them to declare whether or not they were U.S. citizens.

In 2001, the bank had become an indirect subsidiary of a U.S.-based holding company. For purposes of U.S. income tax law, the bank was therefore a "controlled foreign corporation" and was required to comply with applicable U.S. Internal Revenue Service (IRS) regulations on information reporting and tax withholding. Notably, it had to report interest income earned on personal deposit accounts by persons either known to be U.S. citizens or presumed to be U.S. citizens because they had not declared themselves non-U.S. citizens.

The bank mailed an explanatory letter and an account declaration form to all of its personal deposit account holders. The letter indicated that, if an account holder did not declare that he or she was not a U.S. citizen, his or her name and address, as well as the amount of interest income earned, would be disclosed to the IRS. The letter also outlined the purpose for collecting such information and how it would be used.

The complainants alleged that the bank was requiring them to consent to the collection and use of more personal information than was needed to provide account services.

***Our findings***

As far as the substance of the complaint was concerned – that is, the collection and use of personal information – our Office was of the view that the bank was *not* putting foreign legislation ahead of Canadian customers' privacy interests.

As a controlled foreign corporation, the bank was required to comply with applicable IRS regulations. Notably, it had to report the interest income earned by U.S. citizens, but did not have to report that earned by non-U.S. citizens. To ensure provision of accurate information to the IRS and to protect the personal information of non-U.S. citizens, the bank had sent the account declaration form to its account holders, asking them to declare whether they were U.S. citizens or non-U.S. citizens. This was a

reasonable request, for purposes that a reasonable person would consider appropriate in the circumstances, as contemplated by section 5(3) of the Act.

Furthermore, since the bank had identified its purposes and limited the collection of personal information to those purposes, it was also in compliance with Principles 4.2 and 4.4 of the Act.

On this account, the complaint was not well-founded.

### **Quebec company's information-sharing notice not clear enough**

If an organization intends to share customers' names and addresses with third parties for marketing purposes, it must let the customers know, but not just in any old way. Principle 4.3.2 of the Act puts an onus on organizations to make a "reasonable effort" at both bringing purposes to the attention of customers and presenting them in a way the customers can understand.

The company in this case did make an effort, but the question for our Office was, "How reasonable?" The case also has an interesting jurisdictional aspect relating to a transitional provision in *PIPEDA*.

#### ***The facts***

Some months after purchasing beauty products by telephone from a company in Quebec, a complainant had requested in writing that the company remove her name from its mailing list. Several weeks later, in October 2002, her name was still on a list that the company had recently sent to an Ontario consultant hired to trade and rent its customer lists to other organizations.

The complainant's allegation to our Office was that the company had sold her name and address to third parties in Ontario without her consent. She also raised concerns about the company's procedure for allowing customers to opt-out of third-party marketing.

The company explained that the continued appearance of the complainant's name on the mailing list was the result of normal administrative delay in processing the opt-out request. The company also pointed out that its practice of sharing lists of customers' names and addresses with other businesses, as well as its procedure for having one's name removed from the lists, was set out in a document made available to customers in mail-outs and catalogues.

Our investigation confirmed the existence of this document. However, the dominant title on the document was “Money Back Guarantee”, and the notifications in question appeared under the headings “Help Us Conserve Natural Resources” and “Beauty Care is Personal”.

The company removed the complainant’s name from its mailing lists. As a result of our Office’s intervention, the company changed its promotional materials to make them more understandable. Customers can now simply check a box on the purchase order to prevent the sharing of their information. The company also set up a privacy committee, which has adopted a policy on the protection of customers’ personal information and is developing a similar policy for all employees.

The complainant expressed satisfaction with the company’s removal of her name from its mailing lists and with the changes it made to its promotional materials.

### ***Our findings***

Under section 30 of *PIPEDA*, a transitional provision that remained in force for the first three years, the *Act* applied until 2004 to personal information that an organization disclosed outside the province for consideration. Even though the company in question resides in Quebec, our Office agreed to investigate the complaint under the *Act* because the complainant alleged that the company had disclosed her information outside that province for consideration in 2002 – that is, while section 30 was still in effect.

At the time of the complaint, the company’s promotional materials contained a notice stating that customers’ names and addresses were shared with third parties and laying out a procedure for customers to remove themselves from the lists. However, the notice and the removal procedure lacked clarity. The information was hidden away under headings that were not representative of the contents. The notice did not constitute a reasonable effort by the company to ensure that individuals were clearly informed about the secondary disclosure purposes for which the personal information was collected. Therefore, the company was in contravention of Principle 4.3.2 of the *Act*, and the complainant’s consent was not meaningful.

However, since the complainant was satisfied with the outcome of the investigation, our Office concluded that the complaint was resolved.



**Satellite television company alleged to have monitored customers' viewing habits**

When told to keep his satellite system continuously plugged in, the customer assumed the worst of the company. But was its intention really to invade his privacy?

***The facts***

A complainant believed that his satellite television provider was keeping track of what programs he watched. He was convinced that, in requiring customers to keep their telephone lines continuously plugged into receiver boxes, the company's sole purpose was to monitor their viewing habits.

His allegation to our Office was that the company was indiscriminately collecting and using his personal information that it gathered through his telephone connection.

The company confirmed that it does require its satellite customers to keep their telephone lines continuously plugged into the receiver boxes it supplies, but for purposes of billing for pay-per-view and preventing piracy, not monitoring viewing habits. The company explained, and our Office confirmed, that it was not possible with its current technology to monitor any programming other than pay-per-view, since the satellite transmission is one-way only and the receiver boxes are not capable of recording other programs. The only information the company collects is about the packages a customer has purchased and transactions that customers initiate electronically through the pay-per-view ordering system, and it collects such information only for billing purposes.

As for preventing piracy, our Office examined the technical aspects and was satisfied that continuous connection with a live telephone line is effective for this purpose. Despite the company's explanation, the complainant continued to believe it was collecting more information than necessary to prevent piracy, but he could not provide any evidence to support his belief.

***Our findings***

The company's purposes of billing for pay-per-view and preventing piracy were ones that a reasonable person would find appropriate in the circumstances.

There was no evidence that the company was collecting information on subscribers' viewing habits from the telephone connection. Information on program packages and other billing information was collected at the time of purchase, not through a telephone line.

Although the company did collect pay-per-view information through the connection, it did so to meet one of its stated purposes – billing the customer. The continuous connection was also effective in fulfilling the company’s other purpose – preventing piracy.

In sum, the company was collecting and using customers’ personal information to fulfil reasonable purposes and was not collecting or using excessive information for those purposes or any others. The company had complied with Principles 4.4 and 4.5 and section 5(3) of the Act. The complaint was not well-founded.

### **Bank discloses client’s mortgage history to her ex-husband’s lawyer**

“He-said, she-said” cases can be devilishly difficult to adjudicate. In this one, fortunately, a paper trail largely supported what “she said”.

If there’s a lesson for bank staff in this situation, it’s that, when dealing with lawyers, you had better make sure at the outset whose side they’re on.

#### ***The facts***

While attending a court hearing regarding her support arrears action, the complainant had received copies of three documents entered into evidence by her ex-husband’s side: the deed for her home, a land registry office listing of mortgages registered against her home, and a mortgage transaction history.

The complainant believed that the manager of financial services at her bank had given these documents, as well as other information about her financial affairs, to her ex-husband’s lawyer on a certain date. She also held that the manager had admitted as much to her and had asked her not to tell the court about his inappropriate disclosures.

Her allegation to our Office was that the bank had disclosed her personal financial information to her ex-husband’s lawyer.

With respect to the deed and the mortgage listing, our investigation determined that the bank manager would not have had access to these documents on the date in question. Moreover, such documents are publicly available at the land registry office, and evidence indicated that the lawyer had already obtained these two documents from that office when he visited the bank manager.

However, with respect to the mortgage transaction history, documentary evidence established that the lawyer had prepared and sent a summons to the bank manager,

had then written to the manager to make an appointment for the date in question in order to review the documentation demanded on the summons, and had, on the day before the date in question, acknowledged receipt of a reply from the manager. Furthermore, the copy of the complainant's mortgage transaction history that the lawyer submitted to the court had been printed from the bank manager's computer and was dated the same day as his reply to the lawyer.

The manager did not admit to printing the document, providing it to the lawyer, or asking the complainant not to reveal his disclosures. Nevertheless, he did admit that, at first contact, he had mistakenly assumed that the lawyer was acting on the complainant's behalf.

Conceding that the complainant's mortgage transaction history had been disclosed to the complainant, the bank issued her an apology.

### ***Our findings***

The deed of land and the mortgages registered against the complainant's home were determined to be publicly available information obtainable through the land registry office. Such information could be disclosed without knowledge and consent, pursuant to section 7(3)(h.1) of the Act. In any case, it appeared that the lawyer had already gathered this information before approaching the bank.

The mortgage transaction history, however, was determined to have been printed from the bank manager's computer on the same date he had written to the lawyer. Our Office believed, and the bank agreed, that the document had been disclosed without the complainant's consent. The complaint was well-founded.

## **Select Settled Cases under *PIPEDA***

In January 2004, the Office of the Privacy Commissioner introduced a new category of complaint disposition, "Settled during the course of the investigation". A settled case is one in which, during the actual complaint investigation, the Office has helped negotiate a solution satisfactory to all parties, including the Office itself. Of the 379 cases concluded in 2004, 152 (or 40 per cent) fell under the "settled" category.

The following are summaries of several representative settled cases.

### **Laptop lapse by computer store**

When a computer store did not fix a complainant's laptop within a certain time limit, it provided her a new one. Some time later, she was surprised to get a call from a complete stranger, telling her he had just bought a laptop containing her personal information.

As it turned out, the store had repaired the complainant's original computer, and an employee had put it up for resale without examining its contents. The store was able to retrieve the laptop and return it to the complainant. The company also significantly improved its safeguarding policy and practices. Notably, employees now have to not only ensure, but also document, that personal information is completely erased from the hard drives of all computers returned to any of the company's stores across Canada. The company also agreed to implement similar safeguarding procedures for other electronic devices that it sells.

### **Phone and e-mail procedures: One security concern leads to another**

Whenever customers pay their bills through the telecommunications company's interactive voice response system, the system reads back the credit card number and expiry date that the customer entered via the telephone keypad. A complainant was concerned that anyone intercepting a cell phone call could obtain these numbers. But when he e-mailed to express this concern, the company's e-mail reply repeated the account number and personal identification number that he had entered to gain access to the secure account information system. The complainant was now concerned that this sensitive personal information, too, could be available to anyone else who might gain access to the e-mail.

The company reviewed its practices and agreed that it was not necessary to automatically reproduce in e-mail responses the personal data required for accessing the secure site. It has now ceased to include message threads in its e-mail responses to customers. As for the original concern, however, the company pointed out to the complainant that several payment options were available to customers and that, even if credit card numbers were no longer to be read back, customers who chose to pay bills by cell phone would still risk interception of the numbers as they were keyed in.



### **Insurance company fails to heed client's warning**

On two distinct occasions, a complainant had warned his insurance company that unauthorized persons might try to obtain information about life insurance policies he held on his nephews. Despite these warnings, and despite the company's authentication and flagging procedures in place at the time, information was later disclosed to an unauthorized party against the complainant's express wish.

The complainant and the company reached a settlement. As a result of the complaint, the company has greatly improved its authentication and flagging policy and procedures and has incorporated the new policy in its training for customer service representatives.

### **Transportation company eliminates excessive database information**

An employee of a national transportation company complained about lack of security of personal information in an automated crew management system. Specifically, he was concerned that unauthorized personnel, especially union representatives, could gain access to such employee information as date of birth, social insurance number (SIN), health information, wage rates, and vacation eligibility.

In fact, it was not possible for union representatives to gain access to some of the information of concern to the complainant. Moreover, at the time of the complaint, the company had already identified date of birth and the SIN as privacy concerns and was in the process of adjusting its crew management system accordingly. In the end, the company agreed also to remove employees' health information from the system.

### **Personal information circulates on hundred-dollar bill**

When a complainant offered a \$100 bill for a gasoline purchase, the service station attendant asked for identification. According to the complainant, the attendant then wrote his name and driver's licence number on the bill itself, explaining the practice as "company policy" due to the high incidence of counterfeit bills. On reflection after the incident, the complainant worried that his personal information would thus be available to anyone handling the bill for as long as it remained in circulation.

The company does make a policy of having station staff temporarily record identification for customers tendering \$100 bills, but stipulates that the recording be done on separate tracking sheets, not on the bills themselves. Although the attendant

knew the correct procedures and did not admit to having written on the bill, the company took responsibility in the matter, apologized to the complainant, and reached a settlement with him. The company also reminded all its service station employees of the proper procedures for handling personal information.

### **Pharmacy makes consent procedure more customer-friendly**

A complainant objected that his pharmacy was requiring him to sign a consent form before giving him his medication. It seemed to him that the form authorized overly broad disclosure practices, and he was concerned that his personal information might be disclosed for marketing purposes. He also worried that he would not be able to obtain the medications he needed if he refused to sign.

In fact, the pharmacy chain does not disclose customers' personal information to other organizations for marketing purposes. Nevertheless, in response to this and several other complaints about its consent form, the company decided to change the language of the form, making it simpler and easier for customers to understand. The company also implemented a new policy and practice whereby clients who are uncomfortable signing a consent form can provide oral consent to the company's privacy practices, as explained to them by the pharmacist.

### **Another pharmacy clarifies consent policy**

A customer alleged that, even after he had withdrawn his consent to collection, use and disclosure practices, his pharmacy had disclosed personal information to his doctor. He also complained that the pharmacy refused to fill his prescriptions because of his consent withdrawal.

The pharmacy's only record of the complainant's withdrawal of consent was dated some time after the alleged disclosure. After recording the withdrawal, the pharmacy had indeed refused to fill the complainant's prescriptions, but had explained to him at the time that it was company practice not to fill prescriptions for persons who had revoked consent to the collection, use, or disclosure of personal information within the patient's circle of care. The company's privacy literature, however, explained such practice only in general ways, indicating that withdrawal of consent could adversely affect "service". The company agreed to amend its privacy policy to specify that prescriptions could not be filled unless consent was provided.

### **Insurance company welcomes complainant's suggestions about consent form**

An applicant for life insurance complained that the insurance company was requiring her to consent to overly broad collection, use, and disclosure practices.

Our Office facilitated a teleconference with the complainant and the company. The company explained to her its actual practices, which were consistent with the Act. Though the complainant was satisfied with this explanation, the company acknowledged that she had raised a number of important issues about the precision and clarity of its consent language – issues it was taking into account in a current review. The company agreed to send the complainant a copy of its revised form and invited her to make further comments, to be considered in subsequent reviews.

### **An unappreciated birthday announcement**

An employee of a foreign airline's Canadian office complained when a secretary e-mailed his date of birth to fellow employees, despite his previously expressed objection to the local tradition of announcing birthdays. He also alleged that the airline had disclosed his home address and telephone number on lists provided to employees having no need to know such information, and that these lists were not properly safeguarded.

At the suggestion of our Office, airline officials met with the complainant to address the issues he had raised. In the end, the airline resolved the issues to the complainant's satisfaction – notably, by ceasing the practice of announcing birthdays and by taking measures to safeguard and limit access to documents holding employees' personal information. The airline also held privacy briefing sessions with management and administrative staff and posted a privacy notice on an internal bulletin board accessible to all employees.

### **Department store neglects to identify itself as source of mail-out**

Two individuals complained after receiving a mail solicitation ostensibly from a credit monitoring company. Though appearing to have been sent from the company itself, the solicitation indicated an association with a major department store chain with which both complainants held accounts. They both assumed that the chain had given their personal information to the credit monitoring company without their consent. In one case, the complainant had expressly withdrawn consent for the chain to use his personal information for any purpose other than directly conducting business with him.

In fact, the chain had not given personal information to the company. Rather, it had itself had the mail-out notice prepared and sent out, but under the other company's name. The chain's published policy is to rely on opt-out consent for disclosures of customer information to affiliated companies of its own "brand", but it does not disclose to non-affiliated third parties such as the credit monitoring company. In the case of the complainant who had previously withdrawn consent, the chain explained the mail-out as the result of a normal administrative delay in processing his opt-out request.

The chain agreed, however, that it had done a poor job in the marketing campaign and should have clearly indicated that it was acting on the other company's behalf. It also apologized to the complainants, agreed to revise its account application policy to allow new customers to opt-out at the time of enrolment, and undertook a review of its suppression mechanisms to ensure consistency of the opt-out process across all its companies.

### **Non-consensual disclosures to a union**

Several employees complained that a transportation company had forwarded a list of participants in its voluntary separation program to the employees' union without their knowledge and consent. The list included the employees' SINs.

Admitting its mistake, the company changed the application form for severance packages to exclude the requirement for the SIN and to include a statement asking applicants to consent to the release of their personal information to the union.

### **Two cases of envelope mix-ups**

In one case, a complainant had received a student loan notice from her bank – about someone else's loan, not hers. She worried that this other person might be in possession of the same personal information about her as she had received about him – specifically, name, address, SIN, loan number, and loan amount. The mix-up had been the result of simple human error in filling envelopes. No other persons in the complainant's mailing group had received a wrong notice, and the person whose information she had received had not received hers, since he had moved and not left a forwarding address. The bank reached a settlement with the complainant and advised its student centre staff to exercise greater diligence in mailing material to customers.



In the other case, a complainant had received another person's airline ticket in the mail, and that other person had received that of the complainant. The tickets contained personal information in the form of travel itinerary, home address, and telephone number. This mix-up was also the result of human error, in that an airline employee had inadvertently reversed the tickets and envelopes for two phone ticket purchases. The airline apologized to the complainant and reached a settlement with him. It has also reminded its employee to exercise due diligence and care in sending material out to customers.

#### **SINs on display: An overly revealing envelope window**

A pension fund administrator complained that transfer documents he regularly received from a certain bank displayed clients' SINs in the window of the envelopes. Readily acknowledging the problem, the bank instituted a new process whereby both the SIN and the account number were moved from the address portion of the document to an area not visible through the envelope window.

#### **Collection agency corrects inaccurate information**

A complainant had been having difficulty securing credit because of inaccurate information held by a collection agency. He had paid off a debt several years earlier, but the agency had not reported the payment to the credit bureaus. After several unsuccessful attempts through his lawyer to have the information corrected, the complainant approached our Office.

The collection agency had no record of the lawyer's letters. However, after receiving a notice from our Office and yet another letter from the lawyer, the agency looked into the complainant's file, confirmed the debt payoff, and notified the credit bureaus, which amended the complainant's credit files accordingly.

#### **Car dealership refuses credit on erroneous information**

A complainant knew her credit rating was good. When a car dealership turned down the credit application she had cosigned with her son, she wrote the company to ask for the information on which the credit decision had been based. Two months later, she wrote again. Still having received no response after three months, she filed her complaint.

As it turned out, the decision had been based not on her own credit rating, but on her son's. The company had not responded to her access requests because it was unsure

how to do so without disclosing the son's personal information. At our suggestion, the complainant wrote the company another letter, signed by both her and her son and stating that they consented to the disclosure of information about themselves to each other. The company finally responded, indicating that the credit application had been declined because of a bankruptcy entry on the son's credit report. The complainant wrote the company again to advise that the report was in error – the son had not in fact declared bankruptcy, but rather had made a proposal with his creditors and had satisfied its terms more than a year earlier. The company replied that it would use a current credit report for any future application. The complainant was satisfied just to finally have a response from the company.

Meanwhile, the son had managed to lease a car from another dealership under the same brand. In the complainant's words, someone at that dealership "clearly *did* know how to read the credit information."

## **Companies Getting Their Act Together**

### **A lending institution**

A woman complained that a lending institution had disclosed information about her delinquent account to her uncle without her consent.

The complaint had merit, and the institution adjusted the complainant's outstanding account and agreed to send her a letter of apology. During the investigation, our Office noted that the organization had no privacy policies or practices in place. At our urging, it struck a privacy committee, instituted privacy training for employees, and reminded staff to limit the amount of information disclosed in recovering debts.

### **A trucking company**

A former employee alleged that a small, family-owned interprovincial trucking company had disclosed personal information to a creditor without his consent.

There was no evidence to support the allegation, and it came to light that the complainant himself had provided some of the information to the creditor. Nevertheless, our investigation had the effect of educating the company about its obligations under the Act. The company subsequently implemented a written privacy policy, appointed a privacy officer, reviewed its practices regarding employee personal information, and took steps to train employees in proper information handling.

## Incidents under *PIPEDA*

Over and above individual complaints, incident investigations are conducted into matters of improper collection, use or disclosure of personal information that come to the attention of our Office from various sources, including the media, and directly from organizations themselves. They often highlight a systemic issue, or an unrecognized privacy breach that needs to be fixed as soon as possible. Usually, victims are not identified and a formal written complaint has not been filed with the Office.

Last year, the Office completed six incident investigations. Three cases of interest are described below.

### Disclosure of credit reports to fraudster

In March 2004, a credit reporting agency issued a statement that, as a result of a security breach, the credit reports of some 1400 consumers had been disclosed to criminals posing as legitimate credit grantors. The media picked up the story.

The agency's security staff discovered the breach and notified the RCMP, which launched an investigation. It appeared that a single individual committed the breach, and had not been caught as of May 2004.

The agency confirmed that 1398 consumers were affected – 1145 in British Columbia, 163 in Ontario, and 90 in Alberta.

The information disclosed in each credit report was the consumer's name, address, previous address (if available), date of birth, and payment history, as well as creditor names and account numbers, public record items, and collection activity. The agency confirmed that the disclosed information did not include social insurance numbers or bank account particulars.

By way of corrective action, the agency:

- Notified all affected individuals by registered mail;
- Encouraged them to call the agency and review the contents of their credit files;
- Placed an alert message reading "Lost or stolen identification" on their credit files so that creditors would be prompted to ask for additional proof of identity;
- On being contacted by an affected individual, requested that the other major credit reporting agency place a similar message on its credit file for that individual; and

- Offered the affected individuals a free one-year subscription to a credit monitoring service (most accepted this offer).

To address the security problem, the agency put certain fixes in place on its systems. These fixes appear to be effective, in that the same perpetrator attempted to access credit files in the same way a second time, but was blocked.

Since the incident, there have been a small number of fraud attempts involving the disclosed information, but in each case the alerts prevented the fraud.

### **Joint federal/provincial investigation of misdirected medical information**

In July 2004, a newspaper article reported that a married couple had been receiving faxes from various sources containing other parties' personal health information. The couple alleged that they had so notified some of the sources in question, but had continued to receive more of the same.

The Office of the Information and Privacy Commissioner for Alberta originally investigated this incident. That Office determined that, though provincial privacy legislation applied to some of the information transmitted in the faxes, it also appeared to fall under federal jurisdiction under *PIPEDA*. The Office of the Privacy Commissioner of Canada therefore undertook its own investigation in concert with the Alberta office.

The couple in question manages an apartment building. The fax line they use in managing the property has a telephone number similar to that of a health care provider, but with two of the digits reversed. The couple received ten faxes misdialed to their number.

Our Office concerned itself with seven of the ten errant faxes (the other three fell under provincial jurisdiction). Two of the seven were found not to contain personal information. For the remaining five, the sources were determined to be three separate and distinct companies.

The first is a company that owns and operates medical laboratories. The fax it misdirected to the couple's number contained the personal information of an individual who had undergone medical testing by the company. The information included the person's name, age, height, smoking habits, and patient number, as well as a diagnosis and specific medical test results.



In its own internal investigation, this company was unable to determine which of its employees had keyed in the erroneous telephone number, but it did manage to narrow the possibilities down to five. All five employees were aware of the confidential nature of the medical records and the need to ensure against disclosure, and all five had signed a confidentiality oath at the time they were hired, but had not been required to renew the oath since then.

For regularly used fax numbers, this company has now equipped its computers with an electronic automated fax function which checks numbers entered into the system for accuracy before use. For numbers used one time or infrequently (i.e., not programmed into the automated system), the company has provided its employees with a set of instructions to ensure accuracy of transmission. At the Office's request, the company also undertook to revise its policies and procedures to ensure full compliance with the provincial *Health Information Act* and *PIPEDA*.

The second source of the errant faxes is a waste disposal company whose employees are required to have annual medical examinations. This company misdirected three faxes, one of which predated the full implementation of *PIPEDA*. The other two were completed health information forms about two employees who had just had the annual examination. However, it was not the company that had misdirected the faxes, but rather the employees themselves, each misdialing the number in the same way. For privacy reasons, it is the company's practice to have its employees send in their own health forms.

This company has now put the correct fax number on speed dial so that its employees may continue to send in their own health forms with much less risk of inadvertent disclosure. The company also has a privacy officer and acceptable privacy policies in place.

The third company involved is a medical consulting firm whose doctors review and assess new medical consultants' reports on patients. The single misdirected fax in this instance contained such a report that one of the company's doctors had reviewed. The doctor in question had not sent the fax himself, and the company was unable to determine who had. The faxed report contained the patient's name, age, and occupation, as well as a detailed medical history relating to an injury she had sustained in a motor vehicle accident. It also contained information about her children.

When the couple had called to notify this company of the errant fax, a company employee had instructed them to destroy it. In hindsight, the company realized that

this instruction was inappropriate, in that the employee had had no way of confirming that the document was destroyed or whether it was destroyed by a suitable method. The company has arranged to have errant faxes picked up by courier in future. It has also taken procedural measures to have all facsimile numbers verified before transmission and to have any future incidents reported to management.

At our Office's request, this company has informed the patient in question of the disclosure of her personal information, has appointed a privacy officer and has sent the Office copies of its revised fax transmission procedures and privacy policy.

The Office made the following recommendations to the first and third of the companies:

- (1) That the companies implement and follow the Office's recommendations on the transmission of faxes, as set out in the fact sheet entitled "Faxing Personal Information";
- (2) That the companies implement measures to ensure that faxes are recovered if reported as misdirected;
- (3) That the companies notify individuals when their personal information has been inadvertently disclosed as a result of a misdirected fax; and
- (4) That the companies have their employees sign confidentiality/privacy agreements, update such agreements yearly, and review company privacy policies.

### **Credit card receipts blowing in the wind**

In August 2004, a newspaper reported that two women had observed credit card receipts blowing about in their neighbourhood and had traced the source to a local gas station, where old receipts had been placed in a dumpster.

The station owner admitted to having disposed of various receipts from 2002 in the dumpster, but claimed he had been unaware of the privacy implications of this action. He said that the receipts had been contained in boxes, placed in the middle of the dumpster, and covered by other garbage. He suspected that neighbourhood children had climbed into the dumpster and opened the boxes out of curiosity, thereby exposing the receipts to the elements.

He stated that, on being informed of the problem by a reporter on the day in question, he had taken immediate action to gather up the loose receipts, clear the dumpster of

those remaining, and have all the receipts shredded. Though he maintained that he and his employees had been able to find few loose receipts to gather, our investigation established that the two original women witnesses had previously gathered three bags and one boxful of the loose receipts in vicinity of the gas station.

The witnesses turned in the receipts they had gathered to our investigator. A sampling of 1,897 of these documents indicated that most were debit card receipts with no identifiable personal information, and many others were credit card receipts showing a past expiry date. However, a further 151 credit card receipts showed valid (unexpired) account numbers, 16 showed valid account numbers as well as handwritten licence plate numbers, three showed valid account numbers as well as handwritten driver's licence numbers, and one showed both a driver's licence number and a plate number.

The owner gave assurances that he was now aware of his responsibilities under the *Act* and had initiated policies to keep all receipts only for the required six months and then have them destroyed securely by means of shredding.

The owner leases the station from an energy company. In an interview, the company's district manager initially took the position that the company's privacy policy did not apply to its leased establishments. He later conceded, however, that leaseholders were generally expected to adhere to the company's policies and procedures and that the company did customarily provide training and information sessions for leaseholders. But neither he nor the station owner could recall any such information session about privacy policy. The district manager indicated that the company would provide privacy information sessions for leaseholders in the near future, and that he himself would review privacy policies in his monthly meetings with the leaseholders in his district.

Our Office made two recommendations:

- (1) That the company ensure that privacy policies are in place at all of its leased locations and examine the option of putting requirement to that effect into its lease agreements; and
- (2) That the privacy policies for the company's gas stations contain procedures for the proper retention, safeguarding, and disposal of all personal information collected.

## Following Up on *PIPEDA* Case Investigations

In 2004, we introduced a formal procedure of systematic follow-ups to complaint investigations under *PIPEDA*. As a matter of course, the Investigations and Inquiries Branch monitors the progress of organizations in implementing both commitments they make during complaint investigations and recommendations that the Office issues to them in letters of findings. We ask organizations to report on their intentions and their progress in meeting these commitments and recommendations. We also ask them to provide documentary evidence of implementation.

The purpose of follow-up is two-fold. First, it reinforces and clarifies the Office's expectations that organizations take remedial measures in response to specific problems identified in complaint investigations. Second, it provides a reliable ongoing record of organizations' compliance with *PIPEDA*.

In late 2004 and early 2005, in a special exercise to establish a solid basis for such a record, our Investigation and Inquiries Branch applied the new follow-up procedure to past cases in which organizations' responses to recommendations or commitments remained unverified. Specifically, Branch investigators completed follow-ups on over 50 significant unverified cases concluded between January 1, 2001 and November 1, 2004, and involving the federally regulated organizations that had been subject to *PIPEDA* from the beginning (banks, telecommunications companies, national transportation companies, etc.).<sup>3</sup> The subject cases were those in which the Office had identified privacy problems and expected the organizations to take specified remedial action in response either to commitments they had made at our suggestion during investigations or to recommendations we had later made to them in letters of findings.<sup>4</sup>

Through day-to-day dealings, the Office had already formed a good sense of how well respondent organizations had been co-operating in investigations and following through on commitments and recommendations. However, when we analyzed the results of these follow-ups in conjunction with case results already known, we were able to see a fuller, clearer and statistically representative picture of the cumulative effect of our complaint investigations on compliance with *PIPEDA*.<sup>5</sup>

---

<sup>3</sup> The analysis did not include cases involving provincially regulated companies, since such organizations had been subject to the *Act* for less than a year (January 1, 2004).

<sup>4</sup> In the interest of time and efficiency, the many routine cases of (largely resolved) complaints under the access provisions of the *Act* were also excluded from consideration in both the follow-ups and the analysis.

<sup>5</sup> The analysis accounts for approximately 75 per cent of applicable cases concluded during the period in question.

---



Most notably, we determined that, of the verified cases in which our Office expected a remedial response, federally-regulated organizations had fully implemented our recommendations arising out of the investigation of a complaint about nine times out of ten. We also determined that 67 per cent of these satisfactory responses involved some degree of systemic improvement in the organizations themselves. In other words, in approximately two of every three cases, the organization's remedial response had gone beyond the mere settling of a complainant's immediate concern and had led the organization to establish positive substantive change in its information management systems relating to privacy policy, procedures and practices.

The following are just a few examples of systemic improvements implemented by respondent organizations in the first four years of *PIPEDA* arising from our recommendations:

- A bank instituted an alternative process to accommodate deposit account applicants who refused to consent to a credit check.
- Another bank, on our recommendation, collaborated with credit reporting agencies to develop understandable, consumer-friendly formats for credit information.
- Several organizations acknowledged that the use of social insurance numbers (SINs) is a privacy-sensitive issue and changed their policies and practices accordingly. One bank, for example, stopped requiring customers to use a SIN in activating credit cards. Another bank amended its loan application form to indicate that provision of the SIN is optional, and stressed to its employees that the SIN is not required for processing loan applications.
- Through extensive consultation with our Office, a bank whose privacy literature we originally considered to be the least compliant among all the banks greatly improved its consent language and practices, particularly as they related to use and disclosure of personal information for secondary marketing purposes. We now regard this bank's privacy literature as among the best.
- Another bank followed our recommendation to improve the security of computers at its kiosk branches.
- Another bank discontinued its practice of issuing unsolicited credit cards and creating credit card accounts without consent.
- A lending institution struck a privacy committee, instituted privacy training, and instructed staff on limiting the amounts of information they disclose in recovering debts.

- A telecommunications company stopped using customers' telephone records to obtain information about other individuals.
- In a case about the posting of employees' sales records, another telecommunications company told its sales managers about appropriate uses and disclosures of such information, updated its employee training program accordingly, and revised its recruitment and selection process to inform employees of the company's intended uses of their personal information.
- A broadcaster developed and distributed a policy on its use of security cameras and access controls.
- An airline vastly improved its privacy policy and practices related to its rewards program.
- A transportation-related management corporation fully implemented our recommendations concerning its sick leave policy. Most notably, the corporation no longer requires its employees to include specific diagnoses on their medical certificates.
- In close consultation with our Office, a market research company implemented our recommendations regarding its consumer surveys, particularly relating to identification of purposes, and consent to third-party disclosures. The result is a much more transparent and privacy-compliant survey form and process.
- A rewards program not only improved its communications materials as we recommended, but also made other privacy-related improvements beyond our recommendations.

Though not yet complete, the record already abounds with evidence that federally regulated organizations have largely taken their responsibilities under *PIPEDA* very seriously. They have generally cooperated with our Office in complaint investigations and have tended to remedy, in substantive and permanent ways, the problems that we identify. Similarly, the record clearly shows that complaint investigations in themselves greatly increased overall compliance with the *Act* by respondent organizations. Almost half of satisfactory responses by organizations have occurred, not pursuant to recommendations in a letter of findings, but rather during or as a direct result of the complaint investigation itself. In other words, our Office's investigators have been the main instruments of problem solving in almost half the cases of a satisfactory response by an organization.

Our rate of success shows not only the effectiveness of our investigative function, but also the continuing efficacy of the Commissioner's ombudsman role. Although the record appears sound, we are taking measures to improve it. We believe that our new formal procedure of systematic follow-up is one measure in particular that will enable us to bring about an even higher rate of compliance with *PIPEDA*.

# Audit and Review

---

## Strengthening the Audit Function

Section 18(1) of *PIPEDA* allows the Commissioner to audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is contravening the fair information practices set out in the *Act* and Schedule. To date, we have conducted no audits under *PIPEDA*. However, now that *PIPEDA* is fully in force and organizations have had time to adapt to it, our Office has recently begun actions to use the audit power where warranted.

In March 2005, the Branch name changed from “Privacy Practices and Reviews” to “Audit and Review”. This signals an important transformation. Our Office intends to make greater use of audits, and they will become an important tool in carrying out our mandate under both the *Privacy Act* and *PIPEDA*.

The Audit and Review Branch’s goal is to conduct independent and objective audits and reviews of personal information management systems for the purpose of promoting compliance with applicable legislation, policies and standards and improving privacy practices and accountability.

The year 2004 marks the beginning of efforts to rebuild and strengthen audit and review functions. Audits have not yet been used to their potential as among the key tools for addressing the many privacy risks. The systemic risks are wide ranging, including inadequate data security, identity theft, inappropriate gathering, retention and use of personal information, and failure to act when privacy breaches occur.



It will take time to build the capacity to undertake sufficient and appropriate audits. The Branch now has only four auditors to undertake both public and private sector audits. The scope of the “audit universe” is over 150 federal departments and agencies subject to the *Privacy Act*, and thousands of commercial organizations in Canada subject to *PIPEDA*.

Steps our Office will take to strengthen the audit function include:

- Completing an external review of audit methods and practices;
- Setting a Branch goal and articulating team values;
- Undertaking a process to develop a longer term audit strategy and plan in view of privacy risks and issues;
- Building a business case to submit to Treasury Board of Canada to obtain further funding for audit and review;
- Raising awareness with Parliamentary committees about the value of privacy audits;
- Initiating a project to determine and test a process for establishing “reasonable grounds” to select subjects for audits under *PIPEDA*. The criteria and process will be published on our Web site during the next fiscal year, and we will welcome comments;
- Initiating a project to develop a self-assessment tool to help organizations ensure compliance with *PIPEDA*, and to promote good personal information management practices. We want organizations to understand that good privacy makes for good business and that they need a sound privacy management framework. This would include internal auditing of systems and practices for meeting privacy obligations. The self-assessment tool (audit program) will also be published on our Web site; and
- Undertaking a survey of private industry about the use of radio frequency identification devices (RFIDs).

## Keeping Watch on Radio Frequency Identification

We continue to monitor advances in RFID technology. In our view, companies should establish policies and standards before they implement RFID technology, not after the fact. Any use of RFIDs must comply with *PIPEDA*. Furthermore, we want to know the role of RFID applications in data aggregation and mining activities, since these depend on obtaining ever-increasing amounts of detail about individuals and what they buy or rent.

We plan to send letters to selected corporations in Canada that might be introducing RFIDs, to better understand the emerging uses of RFID. Our primary interest is in learning how RFID might be used to link personal information with products and services. We want to know if the technology will be used to identify or track individuals. We also want to know if companies will do privacy impact assessments or threat/risk assessments when developing and implementing RFID applications, and how employees and customers would learn about the presence and use of RFIDs.

The survey results will appear in next year's Annual Report. We will not disclose proprietary business information. We will continue monitoring developments in RFID technology to see where guidance on privacy issues is necessary.



# In the Courts

---

## **PIPEDA Applications**

**U**nder section 14 of *PIPEDA*, an individual complainant has a right, following the Commissioner's investigation and report, to apply to the Federal Court for a hearing in respect of any matter referred to in the Commissioner's report. These matters must be among those identified in section 14. Section 14 also allows the Commissioner to apply directly to the Federal Court in respect of a Commissioner-initiated complaint.

Section 15 also allows the Commissioner to apply directly to the court for a hearing in respect of any matter covered by section 14 (with the consent of the complainant); appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or, with the permission of the Court, appear as a party to any section 14 hearing not initiated by the Commissioner.

Between January 1, 2001 and December 31, 2004, 35 applications were filed in Federal Court in relation to *PIPEDA*. Fifteen of those were filed in 2004. This means that the number of applications in 2004 alone almost equaled all other applications filed since *PIPEDA* came into force until the start of 2004 – a huge annual increase. Following is a list of all of the *PIPEDA* applications filed in the Federal Court in 2004:

- Karen and Daniel Edwards v. Canadian Imperial Bank of Commerce (Federal Court No. T-35-04), Discontinued November 2, 2004
- Keith Vanderbeke v. Royal Bank of Canada (Federal Court No. T-222-04)
- Ron Gass v. NAV Canada (Federal Court No. T-821-04), Dismissed July 2004 (by consent)



- Pierre Jean Trudeau v. Banque TD Canada Trust (Federal Court No. T-851-04), Dismissed February 23, 2005 (for delay)
- Bradley Nazaruk and United Transportation Union, Local 691 v. Canadian National Railways (Federal Court No. T-948-04), Discontinued July 8, 2005
- Janice Morgan v. Alta Flights (Charters) Inc. (Federal Court No. T-1066-04)
- Ian David Kosher v. Canadian Imperial Bank of Commerce (Federal Court No. T-1143-04)
- 3web Corporation v. Llano Gorman (Federal Court No. T-1603-04), Discontinued June 2005
- Paul Wansink and Telecommunications Workers Union v. Telus Communications Inc. (Federal Court No. T-1862-04), Consolidated with Federal Court No. T-1865-04, December 31, 2004
- Henry Fenske and Telecommunications Workers Union v. Telus Communications Inc. (Federal Court No. T-1863-04), Consolidated with Federal Court No. T-1865-04, December 31, 2004
- Paul Bernat and Telecommunications Workers Union v. Telus (Federal Court No. T-1864-04), Consolidated with Federal Court No. T-1865-04 31, December 2004
- Randy Turner and Telecommunications Workers Union v. Telus (Federal Court No. T-1865-04)
- John Testa and Brenda Marie Testa v. Citibank (Federal Court No. T-2135-04), Dismissed June 15, 2005 (settlement reached at pre-trial conference)
- Richard Breithaupt and Peggy Fournier v. Hali MacFarland and Calm Air International ltd. (Federal Court No. T-2061-04)

### **Important Decisions**

Following are important decisions made in 2004 on the application of *PIPEDA*:

#### **Mathew Englander v. Telus Communications Inc. and Privacy Commissioner of Canada**

Federal Court File No. T-1717-01 and Federal Court of Appeal File No. A-388-03

Mr. Englander argued that Telus uses and discloses customers' names, addresses and telephone numbers in its white pages directories and otherwise, without customers' knowledge and consent. He also claimed that Telus inappropriately charges customers for choosing to have their telephone number "non-published". He felt that these actions by Telus contravene sections 5(1) and (3) of *PIPEDA*, as well as several clauses of Schedule 1.

On the question of consent, the former Commissioner found that the company did obtain valid consent through implication and complied with the regulations regarding publicly available information. He focused on the company's questioning of customers about how their information should appear in the white-pages directory and determined that the question itself implied the eventual appearance of the information in publicly available directories. Since information subsequently published in other formats merely reflects what is published in the white pages directory, it too is considered publicly available information for purposes of the regulations under the Act, and may be collected, used or disclosed without consent.

As to charging fees for the non-publication of customers' information, the Commissioner referred to CRTC Telecom Order 98-109, which states that telecommunications companies may charge no more than \$2.00 per month to provide non-published telephone service. He determined that the company did have the authority to charge its monthly fee of \$2.00 for non-publication, and that doing so was not unreasonable.

Mr. Englander filed the very first Federal Court application under section 14 of *PIPEDA* after the former Commissioner released his findings. The former Commissioner was not a party to these proceedings. Ultimately, the Federal Court concluded that Mr. Englander had failed to convince the court that his application was well-founded, and dismissed the application with costs to the Respondent.

Mr. Englander filed an appeal in the Federal Court of Appeal. The current Privacy Commissioner was granted leave to intervene in the appeal.

The Court heard the appeal on October 7, 2004. The decision, released on November 17, 2004, allowed the appeal in part on the basis that Telus did not have proper informed consent from first-time customers to use their personal information in directories; consent is not informed when the person allegedly giving it is not aware at the time of the possibility of opting-out. Information given to customers subsequently may factor into an evaluation of compliance with the "openness" principle, but comes too late for consent. The Court emphasized that consent in this situation was particularly critical because it was the gateway to information becoming publicly available.

The Court's February 9, 2005, decision declared that in light of Telus' undertaking to change its practices to conform with *PIPEDA*, there was no need to compel Telus to make those changes. The judgment states that "the Court is satisfied that it is sufficient in the case at bar to declare that Telus has infringed section 5 of the *Personal*

*Information Protection and Electronic Documents Act* and that there is no need for the issuance of a mandatory injunction.”

**Erwin Eastmond v. Canadian Pacific Railway and Privacy Commissioner of Canada**

Federal Court File No. T-309-03

Mr. Eastmond complained that his employer was collecting the personal information of employees without their consent. Specifically, he was concerned that digital video recording cameras installed at the company yard could collect personal information of employees.

The former Privacy Commissioner applied section 5(3) of *PIPEDA* and explained that when using this section one must consider both the appropriateness of the organization's purposes for collection and the circumstances surrounding those purposes. To that end, he used a four-point test for assessing reasonableness: (1) Is the measure demonstrably necessary to meet a specific need; (2) Is it likely to be effective in meeting that need; (3) Is the loss of privacy proportional to the benefit gained; and (4) Is there a less privacy-invasive way of achieving the same end? The former Commissioner found that a reasonable person would not consider these circumstances to warrant such an intrusive measure as digital video surveillance. He concluded that the company's use of this type of surveillance for their stated purposes was not appropriate and that the company had contravened section 5(3) of *PIPEDA*.

In February 2003, Mr. Eastmond filed an application, as permitted by section 14 of *PIPEDA*. He sought an order confirming the finding of the former Commissioner as well as various related orders. He also requested a certified copy of the former Commissioner's record of investigation.

The former Commissioner objected to this request for materials, and the Court agreed in June 2003 that the *Federal Court Rules* do not allow an Applicant, in a section 14 application under *PIPEDA*, to request material in the possession of the Privacy Commissioner.

The Interim Privacy Commissioner was also added as a party pursuant to section 15(c) of *PIPEDA*, but took no position as to the appropriate outcome on the facts, instead arguing on points of law that the Court should accord some deference to the expertise of the Commissioner and should adopt the four-point test to determine the appropriateness of the collection of the information by CP Rail. A supplementary factum was filed in December 2003 addressing the jurisdiction over the issues of

both the Commissioner and the Court, notwithstanding that these issues arose in a collective bargaining situation. The supplementary factum suggested that concurrent jurisdiction existed in this situation.

The application was heard in April 2004. On June 11, 2004, the court released its decision. The Court found that the Privacy Commissioner did have jurisdiction, that the essence of this dispute did not arise from the collective agreement, and that it was not Parliament's intention to exclude unionized workers from the scope of *PIPEDA*.

The Court also concluded that although this was a proceeding *de novo*, the Commissioner was entitled to a degree of deference in light of the Commissioner's expertise.

Finally, the Court adopted the four-point test for section 5(3), with the caveat that the specific factors considered in this case might not be appropriate in all cases. Using that test, the Court concluded that a reasonable person would consider the organization's purposes for collecting the images through the medium of a digital video camera to be appropriate in the circumstances. CP Rail therefore had not contravened *PIPEDA*.

### **Cases in the Courts**

**The following cases are of particular interest in the ongoing interpretation of PIPEDA:**

#### **Keith Vanderbeke v. Royal Bank of Canada**

Federal Court File No. T-222-04

Mr. Vanderbeke had previously made a complaint about Royal Bank of Canada's (RBC) treatment of his personal information. This related complaint alleged systemic improprieties in RBC's record keeping procedures, specifically that the bank was not "properly" retaining mortgage renewal acknowledgement letters for its clients. The bank explained that they do not keep a copy of the acknowledgement letters sent to customers as the letters contain information that is available in other documents. Reviewing the complaint, the Assistant Privacy Commissioner considered that *PIPEDA* provides individuals with a right of access to personal information itself, but not necessarily the specific documents containing that information. Accordingly, she considered the complaint not well-founded.

Mr. Vanderbeke filed an application, as permitted by section 14 of *PIPEDA*, on January 29, 2004. RBC made a motion for an order to strike the application, but was not successful.



An order dated July 5, 2004, stipulated that Mr. Vanderbeke pay security monies into Court before filing his affidavit. This caused delay in the proceedings until February 23, 2005. To date, the Commissioner has not become involved in this application, but is monitoring developments closely.

**Janice Morgan v. Alta Flights (Charters) Inc. and Privacy Commissioner of Canada**

Federal Court File No. T-1066-04 and Federal Court of Appeal File No. A-184-05

Ms. Morgan, a former employee of Alta Flights, complained that her employer tried to collect and use her personal information without her knowledge and consent. Specifically, she alleged that a manager had taped a digital recorder to the underside of a table in a smoking room accessible to employees in an attempt to collect their personal information. The company acknowledged that the manager had attempted to collect employee personal information without the knowledge or consent of those employees.

The investigation determined that since there was no evidence of a recording, there was no evidence that the complainant's personal information had been collected or used. The Assistant Privacy Commissioner concluded that the company was not in contravention of *PIPEDA* and, accordingly, the complaint was not well-founded. However, she cautioned that the company should not interpret her finding as an approval of what the manager had attempted to do.

Ms. Morgan filed an application in Federal Court, as permitted by section 14 of *PIPEDA*, on May 26, 2004. The original application incorrectly named the Privacy Commissioner as a respondent. On September 14, 2004, the Court granted the Privacy Commissioner's motion to be struck as a respondent and added as a party to the application, as permitted by section 15(c) of *PIPEDA*.

At trial, the Privacy Commissioner made representations concerning five matters: (1) jurisdiction of *PIPEDA* over the subject matter notwithstanding a *Canada Labour Code* unjust dismissal complaint in respect of the same issue; (2) the appropriate standard of review and deference to be accorded the Privacy Commissioner's findings; (3) the appropriate interpretation of section 7(1)(b); (4) whether an attempted collection constituted a collection; and (v) whether there is a common law jurisdiction to grant remedies not authorized by *PIPEDA*.

The court heard the application on March 15, 2005. Like the Assistant Privacy Commissioner, the Court concluded that since there was no evidence that any conversations were recorded, the company did not actually manage to collect and/or

use any personal information. There was no violation of *PIPEDA* since an attempt to breach the *Act* does not exist as a violation of *PIPEDA*.

On the issue of whether to give deference to the Privacy Commissioner's decision, the Court concluded that it may rely on the decision of the Privacy Commissioner or certain parts of it in arriving at its determination, but it is not bound to do so. When exercising its discretion *de novo*, the Court will give less deference to the decision of the Privacy Commissioner than it would otherwise. However, some regard is warranted about the factors taken into consideration by the Privacy Commissioner in balancing the privacy interests of the complainant and the employer's legitimate interest in protecting its employees and property.

Ms. Morgan filed an appeal of the decision in April 2005.

**Paul Wansink and Telecommunications Workers Union v. Telus and Privacy Commissioner of Canada**  
Federal Court File No. T-1862-04

**Henry Fenske and Telecommunications Workers Union v. Telus and Privacy Commissioner of Canada**  
Federal Court File No. T-1863-04

**Paul Bernat and Telecommunications Workers Union v. Telus and Privacy Commissioner of Canada**  
Federal Court File No. T-1864-04

**Randy Turner and Telecommunications Workers Union v. Telus and Privacy Commissioner of Canada**  
Federal Court File No. T-2222-03

The Applicants complained to the Privacy Commissioner that their employer, Telus Communications Inc., had contravened *PIPEDA* by forcing them to consent to the collection of personal biometric information and to provide the information to enable a computer to automatically authenticate identity using their voice prints.

The Assistant Privacy Commissioner assessed the requirement of the voice print and found it not overly invasive. She found it an appropriate balance between the employees' right to privacy and the employer's needs. The purpose was reasonable and appropriate, Telus had properly informed its employees of the purposes, and it had appropriate safeguards in place in relation to the information.

After the release of the Assistant Commissioner's findings, each of the four complainants filed a separate application in Federal Court under section 14 of *PIPEDA*. An order dated December 31, 2004 consolidated all of the applications under Federal Court File No. T-1865-04.

The Privacy Commissioner then sought under section 15(c) of *PIPEDA* to become a party to these applications in order to make representations to assist the court in developing a test for negotiating the balance between commercial needs and individual privacy rights. Telus consented to the motion but made representations to the Court suggesting a limited role for the Privacy Commissioner. The Commissioner successfully challenged this, and on February 22, 2005, obtained full party status.

The Commissioner made representations on several matters, including: (1) that the Telecommunications Union was not a proper applicant in the proceeding; (2) that the Court should have due regard for the factors to be considered in balancing the interests of the parties; (3) that the legal framework and factors used by the Commissioner in balancing the interests of the parties should be applied by the Court; (4) that *PIPEDA* does not require that the employer seek union consent rather than seeking consent directly from individual employees; (5) that exceptions to consent requirements do not apply in this situation; (6) when may consent be implied; and (7) a recognition of the ability to withdraw consent.

A hearing has been scheduled for September 20, 2005.

**John Testa and Brenda Marie Testa v. Citibank**

Federal Court File No. T-2135-04

Mr. Testa claimed that Citibank disclosed a significant amount of his personal information to his employees without his consent. He further alleged that these disclosures were extremely damaging to his reputation and contributed to his decision to resign as the head of the company.

In her finding, the Assistant Commissioner acknowledged that *PIPEDA* allows an organization to disclose an individual's personal information without consent for the purposes of collecting a debt. However, this exception did not confer *carte blanche* for an organization to disclose however much information it wished. She felt that in this instance it was clear that excessive amounts of information had been divulged. Accordingly, she found the bank to be in contravention of Principle 4.3 of Schedule 1 of *PIPEDA* and the complaint to be well-founded.

An application was filed in Federal Court on December 1, 2004. The Commissioner was expected to seek leave to appear as a party as permitted by section 15(c) of *PIPEDA*. However, a settlement was reached at a pre-trial dispute resolution conference and, accordingly, the application was dismissed on June 15, 2005.

**Richard Breithaupt and Peggy Fournier v. Hali MacFarlane and Calm Air International Ltd.**

Federal Court File No. T-2061-04

Mr. Breithaupt complained that a Calm Air employee (Ms. MacFarlane) disclosed his and his wife's itinerary information to the RCMP without their knowledge and consent. It was undisputed that the Calm Air employee had obtained access to the information without their knowledge and consent. However, both the Calm Air employee and the RCMP officer denied that the employee disclosed this information to the officer.

Documentary evidence led the Assistant Commissioner to conclude that there was indeed a disclosure. She found that the employee had used personal information for purposes other than those for which it was collected, and then disclosed it in contravention of Principles 4.3 and 4.5 of Schedule 1 of *PIPEDA*. Accordingly, the complaint was well-founded.

The complainant filed an application under section 14 of *PIPEDA* in Federal Court on November 18, 2004. The Commissioner is not a party to this application, though she is monitoring its progress.

## Judicial Review

The following cases are important in defining the extent of the Commissioner's enforcement powers under *PIPEDA*:

**Blood Tribe Department of Health v. Privacy Commissioner of Canada et al.**

Federal Court File No. T-2222-03 and Federal Court of Appeal File No. A-147-05

A complaint was filed with our Office alleging (among other things) that the Blood Tribe Department of Health had denied an individual access to her personal information and did not provide reasons for the denial.

In our view, the Commissioner must have access to all documents to ensure that exemptions claimed have been properly applied and to guard against abuse. However, during this investigation the Blood Tribe Department of Health refused to provide the Commissioner with access to solicitor-client privileged documents. As a result, our Office issued its first order for the production of records, using the enforcement powers as set out in sections 12(1)(a) and (c) of *PIPEDA*.



In response, an application for judicial review of the Privacy Commissioner's decision to issue an order for production was made by the Blood Tribe Department of Health, as permitted by section 18.1 of the *Federal Court Act*. The Court dismissed the application in March 2005. Mr. Justice Mosley stated that when the Privacy Commissioner is seized with a complaint over the retention and use of personal information, she has the responsibility to determine the facts and the duty to prepare a report of her findings. She cannot effectively perform that role if she is denied access to the information necessary to ascertain the facts merely because a claim of privilege is made. The Court was satisfied that the Commissioner had correctly exercised her authority to issue the production order. The order did not limit or deny any solicitor-client privilege that the applicant may enjoy in the questioned documents.

The Applicant filed an appeal of this decision in April 2005.

**3web Corporation v. Llano Gorman and Privacy Commissioner of Canada**  
Federal Court File No. T-1603-04

Mr. Gorman complained that 3web Corporation, an internet service provider who had been his employer, had installed web-cameras to monitor employees in the workplace. The cameras were located in the sales and marketing division and the technical support staff area. The Assistant Commissioner concluded that the complaint was well-founded. In doing so, she stated that: (a) it was unlikely that a reasonable person would consider employee productivity to be an appropriate reason to use video and audio surveillance; and (b) by using web cameras in the manner described in this complaint, the company was not fundamentally recognizing the right of privacy of its employees; the balance integral to section 3 of *PIPEDA* was tipped too far away from the privacy rights of individuals. The use of cameras for these purposes would undermine *PIPEDA*.

*PIPEDA* provides that a complainant or the Privacy Commissioner may apply to the Federal Court for a hearing of any matter referred to in the Commissioner's report. In that the Commissioner's report makes recommendations only, there is no such provision for a respondent organization. In this case, the organization initiated a judicial review application. It named Mr. Gorman as a respondent, although it also sought an order stating that the Assistant Privacy Commissioner's report was "illegal and invalid."

In October 2004, the Privacy Commissioner filed a motion requesting that (a) she be added as an intervener and (b) the application be struck. This motion was heard

in February 2005, at which time the Commissioner was added as an intervener to the proceeding. The Court dismissed the Commissioner's motion to strike the application as a whole, concluding that the issue was best suited for determination at trial.

The company discontinued the proceeding in June 2005.



# Public Education and Communications

The Office of the Privacy Commissioner of Canada is mandated specifically under *PIPEDA* to develop and conduct information programs to foster public and organizational understanding and recognition of the rules that govern the collection, use and disclosure of personal information. And although there is no legislative mandate for public education specified under the *Privacy Act*, there is certainly a mandate to ensure departments and agencies are held accountable for their personal information handling practices. There is often a necessity to inform the public, as well as departments and agencies, about the requirements of the Act and related policies, and the impact on the privacy rights of Canadians of current and proposed government activities.

In 2004, the Office undertook a strategic communications planning effort with the expertise of external consultants, and the result was a comprehensive communications and outreach strategy for the coming years. This strategy will enable the Office to have a more comprehensive, proactive approach to communications planning and delivery; a more truly public education-focused approach to communications surrounding *PIPEDA*; and build a greater level of awareness of the Office and of key privacy issues under both laws.

In addition to developing this strategy the Office undertook the following communications activities in 2004:

## **Speeches and Special Events**

Speaking engagement opportunities have helped our Office raise awareness of privacy issues among diverse audiences and settings, including professional and industry associations, non-profit and advocacy groups and universities. In 2004, the Commissioner, Assistant Commissioners and other senior officials delivered



19 speeches, speaking out about issues with privacy implications, such as security initiatives and health care delivery.

In March 2004, the Office began hosting an in-house Lecture Series (approximately one per month). These information sessions featured experts on a variety of privacy issues and brought together members of the privacy community and staff. In 2004, the Office hosted ten of these information sessions.

### **Media Relations**

Privacy issues continued to be of interest to the media in 2004, with significant coverage in Canada on issues such as the full implementation of *PIPEDA*, about which the Office received media calls and participated in interviews. In addition, through other proactive media relations efforts, such as the dissemination of news releases, the Office had the opportunity to raise awareness of, for example, the launch of its Contributions Program; the Commissioner's views on important legislation, such as the *Public Safety Act* and the do-not-call list legislation; and the Office's views regarding transborder flows of personal information.

### **Web Site**

We post new and useful information on our Web site on an ongoing basis. Fact sheets, news releases, speeches, case summaries of findings under *PIPEDA*, are posted to keep the site interesting to individuals and organizations. In 2004-2005, the Office redesigned its Web site in order to make it compliant with the Common Look and Feel standards established by Treasury Board. This resulted in an enhancement to the design as well as to the navigation tools on the site, in order to help visitors make better use of the site. The Office also made the site more dynamic with the posting of a downloadable Web-video for businesses on complying with *PIPEDA*. Since 2001, we are pleased to report that visits to the site have more than quadrupled, reaching 922,106 in 2004.

### **Publications**

The Office has produced information materials, including guides for individuals and organizations on *PIPEDA*, as well as a variety of new fact sheets on issues including consent, use of the social insurance number in the private sector, transborder flow of personal information, and how our Office conducts investigations into potential privacy breaches.

In 2004-2005, in addition to preparing new fact sheets, we developed an e-kit for businesses to help them comply with the new law. We also revised the content of our guides, to ensure they were up-to-date given the final stage of implementation of *PIPEDA* on January 1, 2004. We received requests for these materials on a daily basis. Not only were these materials sent to individuals upon request, they were also distributed at conferences and special events, and accessed in electronic format by visitors to our Web site. In 2004, close to 22,000 of our publications (guides, fact sheets, annual reports, copies of both federal privacy laws) were sent out, in addition to the more than 742,000 publications which were downloaded from our Web site.

### **Internal Communications**

Internal communications activities were also a focus of the Office and played a key role in 2004, increasing transparency between management and staff, especially during its ongoing institutional renewal, but also through day-to-day activities. Internal communications activities in 2004 involved providing staff with information on, for example, human resources issues, upcoming speaking engagements, Parliamentary appearances, senior management and labour management committee meetings, and special events such as all-staff meetings and information sessions. The Office has been developing an Intranet, an internal communications portal to host all internal communications and maximize staff access to information, which will be launched in 2005.

In the upcoming year, the Office will continue to undertake the activities outlined above. We also hope to be in a position to initiate many of the more proactive public education activities outlined in the communications and outreach strategy.



# Corporate Services

---

## On the Path to Institutional Renewal

**T**he Commissioner's most immediate priority has been to lead the Office's institutional renewal by strengthening OPC management processes, particularly human resources and financial management – planning, budgeting, reporting and control mechanisms.

The overall financial framework in which our Office operates is based on the government fiscal year (2004-2005).

### Planning and Reporting

A foundation component of the Office's institutional renewal is a strategic planning, reporting and control process. During 2004-05 we completed our first year under this revised process. The strategic plan established at the beginning of the year was our road map for the year. As part of the new process were reporting and review opportunities. We made adjustments to plans and budgets throughout the year. To assist in our reporting and reviews we developed a Performance Measurement Framework and a monthly performance report. We also launched a Business Process Review of the entire organization which will enable the Office to better estimate resource requirements and to draft a business case for permanent funding.

### Human Resources

We continue to work toward the development and implementation of changes to improve how the office is run and the quality of the workplace. Significant changes and improvements have been made to the Human Resource management policies and practices.



We developed a number of Human Resource policies in consultation with central agencies and unions. These policies will guide us as we build on the successes of the past year and we continue on our path of institutional renewal. An Instrument of Delegation of Human Resource Management was developed and will serve as a tool to inform and guide managers, and enable them to manage their human resources. A new Strategic Human Resource Plan and Staffing Strategy, as well as an Employment Equity Action Plan, will help the OPC achieve its mandate and ensure the recruitment of a highly qualified workforce that is diversified and representative of Canadian society. As part of OPC's commitment to increase transparency in the staffing processes, a staff newsletter was developed; it is distributed on a monthly basis to all staff.

Over the course of the past fiscal year we made significant strides in the area of organizational learning, including the development of a learning strategy with the Canada School of Public Service (CSPS), training and information sessions in values based staffing, language training sessions, performance management and employee appraisals and harassment in the workplace. The development and implementation of a Learning Strategy and Curriculum with the CSPS will enable staff to continue to develop the expertise and competencies required to fulfil their functions, as well as to position staff to take on new responsibilities and accountabilities.

We continued to work collaboratively with Central Agencies such as the Public Service Commission and the Public Service Human Resources Management Agency of Canada on follow-up measures to the recommendations of the Public Service Commission and the 2003 report of the Auditor General of Canada. This included measures that will allow OPC the opportunity to regain its full staffing delegation authority.

### **Finance and Administration**

The OPC received a clean opinion on Audited 2003-2004 Financial Statements by the Office of the Auditor General of Canada. This is a significant milestone and a very positive indicator that the organization has indeed advanced on the path of institutional renewal. The organization has built on that success by establishing planning and review cycles, by streamlining and improving the financial management policies and practices.

### **Information Management / Information Technology**

Significant advancements have also been made in how we manage our information assets. We completed an audit of our information management systems and we

completed a vulnerability assessment of our information technology. We also completed an information technology strategy. This will help us to not only meet our obligations with respect to the management of government information and security policies, but more importantly it will guide us as we move forward in improving on the management of our information assets. During the year we completed a significant upgrade to our case tracking and reporting system, Integrated Investigations Application (IIA). Finally we also established the framework for an internal Intranet site. This site will allow for effective communicating and sharing on information for employees.

### **Down the road**

Strategic planning is an important annual exercise for the OPC. Our last session in January 2005 provided managers and employees an opportunity to re-examine the OPC's priorities for 2005-2006, and the actions they would take to achieve these priorities.

Corporate Services priorities for 2005-2006 are to:

- Develop and implement a Management Accountability Framework (MAF);
- Implement and maintain a human resource strategy that enables the Office to recruit, retain and develop staff and foster a continuous learning environment;
- Satisfy central agencies' requirements to regain delegated authorities, and enable the Office to take on new delegation to implement the Public Service Modernization Act;
- Develop and implement integrated information management;
- Complete Business Case for Resources for the OPC;
- Review Corporate Services Branch and Human Resources Branch policies and procedures; and
- Continue providing effective integrated financial services to the OPC.

### **Our Resource Needs**

At the beginning of fiscal year 2004-2005, the Office's budget was \$11.2 million, the same as the previous year. Included was \$6.7 million for the Office's *PIPEDA* activities. Ongoing funding of OPC activities continues to be extremely important.

With privacy rights continually under threat, the Office's operations need to be funded adequately so that it is prepared to address the multitude of emerging privacy issues in the public and private sector.

The Office does not have adequate resources to fully exercise its powers and responsibilities under both Acts. Without adequate permanent funding, the Office cannot:

- Reinforce our audit and review functions to effectively address compliance under both privacy laws or strengthen our capacity to monitor, research and respond to emerging issues of technology and privacy;
- Conduct outreach and public education to influence change so policies and programs are viewed through a privacy lens;
- Continue investigating in a timely manner and resolving the growing number of complaints under both Acts; and
- Continue providing specialized legal and strategic advice and litigation support under both federal privacy laws, as well as strengthening established approaches and procedures to deal with cross-jurisdictional complaints.

To this end, the Office's priority beginning in the last quarter of fiscal year 2004-05 was to completely review all business processes. The review included establishing workload indicators and reviewing the legislative requirements, as well as external and internal factors that have an impact on our operations. This will enable the Office to develop a Business Case and make a formal submission to the Treasury Board Secretariat and to Parliament later in 2005 to stabilize our resource base and seek permanent funding for the Office.

We hope that with adequate permanent funding, the Office can further assure Parliament that it is effectively ensuring respect for Canadians' privacy rights in the public and private sectors.

## Financial Information

April 1, 2004 to March 31, 2005

	<b>Expenditure Totals (\$)</b>	<b>% of Totals</b>
<i>Privacy Act</i>	3,745,058	32
<i>PIPEDA</i>	6,849,650	58.5
Corporate Services	1,107,296	9.5
<b>Total</b>	<b>11,702,004</b>	<b>100</b>

Note: Although OPC salary budget allows for approximately 100 FTEs (full-time equivalents), there were only 86 FTEs staffed at the Office at the end of March 2005.

<b>Detailed Expenditures<sup>(1)</sup></b>	<b><i>Privacy Act</i></b>	<b><i>PIPEDA</i></b>	<b>Corporate Services</b>	<b>Total</b>
Salaries	3,330,147	3,039,732	419,120	6,788,999
Employee Benefits Program	190,327	844,575	154,640	1,189,542
Transportation & Communication	41,238	266,129	81,282	388,649
Information	1,907	147,911	5,239	155,057
Professional Services	171,783	1,397,579	210,403	1,779,765
Rentals	2,730	107,874	23,759	134,363
Repairs & Maintenance	4,698	155,805	85,353	245,856
Materials & Supplies	9,304	50,764	21,633	81,701
Acquisition of Machinery & Equipment	384	451,788	98,026	550,198
Other Subsidies & Payments	- 7,460	20,084	7,841	20,465
Transfer Payments	0	367,409	0	367,409
<b>Total</b>	<b>3,745,058</b>	<b>6,849,650</b>	<b>1,107,296</b>	<b>11,702,004</b>

<sup>(1)</sup> Total expenditure figures are consistent with the Public Accounts of Canada.

### **Financial Statements**

The Management Responsibility letter and the audited financial statements as at March 31, 2005 will be available on our Web site at [www.privcom.gc.ca](http://www.privcom.gc.ca) in October 2005.







Renseignements financiers

Du 1<sup>er</sup> avril 2004 au 31 mars 2005

Dépenses globales (\$)	Loi sur la protection des renseignements personnels	LPRPDÉ	Gestion intégrée	Total
% du total				
32	3 745 058	6 849 650	1 107 296	11 702 004

Note : Bien que le budget salarial du CVP ait permis environ 100 ETP (équivalent temps plein), le Commissariat ne comptait que 86 employés à temps plein à la fin de mars 2005.

Dépenses détaillées <sup>(1)</sup>	Loi sur la protection des renseignements personnels	LPRPDÉ	Gestion intégrée	Total
Salaires et traitements	3 330 147	3 039 732	419 120	6 788 999
Cotisations au régime d'avantages sociaux des employés	190 327	844 575	154 640	1 189 542
Transports et communications	41 238	266 129	81 282	388 649
Information	1 907	147 911	5 239	155 057
Services professionnels	171 783	1 397 579	210 403	1 779 765
Locations	2 730	107 874	23 759	134 363
Réparations et entretien	4 698	155 805	85 353	245 856
Approvisionnement et fournitures	9 304	50 764	21 633	81 701
Achat d'appareils et d'équipements	384	451 788	98 026	550 198
Autres subventions et paiements	- 7 460	20 084	7 841	20 465
Transfer Payments	0	367 409	0	367 409
<b>Total</b>	<b>3 745 058</b>	<b>6 849 650</b>	<b>1 107 296</b>	<b>11 702 004</b>

<sup>(1)</sup> Les dépenses globales correspondent aux données des Comptes publics du Canada.

États financiers

La lettre de responsabilité de la direction à l'égard des états financiers et les états financiers vérifiés en date du 31 mars 2005 pourront être consultés sur notre site Web [www.privcom.gc.ca](http://www.privcom.gc.ca) en octobre 2005.

Compte tenu des menaces constantes à l'endroit du droit à la protection de la vie privée, les activités du Commissariat doivent être adéquatement financées de façon à ce que ce dernier prenne des mesures pour traiter la multitude des nouveaux enjeux en matière de protection de la vie privée dans les secteurs public et privé.

Le Commissariat ne possède pas les ressources adéquates pour exercer pleinement ses pouvoirs et assumer ses responsabilités en vertu des deux lois. Sans financement permanent suffisant, le Commissariat n'est pas en mesure de :

- renforcer ses fonctions de vérification et d'examen de façon à traiter efficacement l'application des deux lois régissant la protection des renseignements personnels, ou renforcer notre capacité de surveillance, de recherche et de réponse aux nouveaux enjeux en matière de technologie et de protection de la vie privée ;
- mener des activités d'information et de sensibilisation du grand public afin d'influer sur les changements pour que les politiques et programmes soient perçus selon un leitmotiv respectant la protection de la vie privée ;
- continuer à mener des enquêtes en temps opportun et à régler un nombre de plus en plus élevé de plaintes en vertu des deux lois ;
- continuer à fournir des avis juridiques et stratégiques ainsi qu'un soutien juridique en vertu des deux lois régissant la protection des renseignements personnels, et renforcer les méthodes et procédures établies pour régler les plaintes entre les différentes juridictions.

À cette fin, la priorité du Commissariat au cours du dernier trimestre de l'exercice 2004-2005 a consisté à mener à terme un examen de ses processus opérationnels à l'échelle de l'organisme. Il a donc fallu, notamment, établir des indicateurs de charge de travail et revoir les exigences législatives ainsi que les facteurs, tant internes qu'externes, qui ont une incidence sur les activités du Commissariat. Cela permettra au Commissariat d'élaborer une analyse de rentabilisation et de déposer un document de présentation officielle au Secrétaire du Conseil du Trésor et au Parlement plus tard en 2005, en vue de stabiliser les ressources dont il dispose et de demander un financement permanent.

Nous espérons qu'avec un financement permanent, le Commissariat sera en mesure d'offrir une assurance renouvelée au Parlement pour veiller au respect du droit des Canadiennes et des Canadiens à la protection de leurs renseignements personnels dans les secteurs public et privé.



## Gestion de l'information et technologie de l'information

Des progrès considérables ont également été accomplis en ce qui a trait à la gestion de nos ressources d'information. Nous avons terminé la vérification de nos systèmes de gestion de l'information ainsi qu'une évaluation de la vulnérabilité de notre technologie de l'information. Nous avons également élaboré une stratégie en matière de technologie de l'information. Cela nous aidera non seulement à remplir nos obligations dans le cadre de la gestion des renseignements administratifs et des politiques en matière de sécurité mais, surtout, à nous guider pendant que nous procédons à l'amélioration de la gestion de nos ressources d'information. Au cours de l'année, nous avons considérablement amélioré notre système de suivi des dossiers et d'établissement des rapports, l'Application d'enquête intégrée (AEI). Finalement, nous avons également mis au point un cadre pour un site intranet interne. Ce site permettra aux employés de communiquer et d'échanger des renseignements efficacement.

### Pour l'année qui vient

La planification stratégique est un exercice annuel important au CPVP. Notre dernière session, en janvier 2005, a permis aux gestionnaires et aux employés de réexaminer les priorités du Commissariat pour 2005-2006, ainsi que les actions qu'ils entreprendront pour les mener à bien.

### Gestion intégrée – priorités pour l'exercice 2005-2006 :

- élaborer et mettre en œuvre un cadre de responsabilisation de gestion (CRG) ;
- mettre en œuvre et maintenir une stratégie en ressources humaines qui habilitera le Commissariat à recruter, à conserver et à former le personnel, de même qu'à favoriser un environnement d'apprentissage continu ;
- satisfaire aux exigences des organismes centraux afin de recouvrer les pouvoirs délégués et de permettre au Commissariat d'assumer une nouvelle délégation afin d'appliquer la *Loi sur la modernisation de la fonction publique* ;
- élaborer et mettre en œuvre la gestion intégrée de l'information ;
- rédiger une analyse de rentabilisation des ressources pour le CPVP ;
- examiner les politiques et les processus de la Direction de la gestion intégrée et de la Direction des ressources humaines ; et
- continuer à procurer des services financiers intégrés efficaces au CPVP.

### Besoins en matière de ressources

Au début de l'exercice 2004-2005, le budget du Commissariat s'établissait à 11,2 millions de dollars, soit le même montant que celui de l'exercice précédent. De cette somme, 6,7 millions de dollars visent les activités du Commissariat à l'égard de la LPRPDE. Le financement des activités du CPVP est toujours un enjeu capital.

Nous avons élaboré un certain nombre de politiques en matière de ressources humaines, en consultation avec des organismes centraux et des syndicats. Ces politiques nous guideront pendant que nous tirons profit de nos succès de la dernière année et que nous poursuivons notre cheminement vers le renouvellement institutionnel. Nous avons établi un instrument de délégation en matière de gestion des ressources humaines qui nous servira à informer et à aiguiller les gestionnaires et permettra à ceux-ci de gérer les ressources humaines. Un nouveau plan stratégique en matière de ressources humaines et une stratégie de dotation ainsi qu'un plan d'action sur l'équité en matière d'emploi aideront le CPVP à respecter son mandat et à assurer le recrutement d'effectifs hautement qualifiés, diversifiés et représentatifs de la société canadienne. En vertu de l'engagement du CPVP à faire preuve d'une meilleure transparence dans le processus de dotation, un bulletin du personnel a été mis sur pied ; il est distribué chaque mois à tout le personnel.

Tout au long du dernier exercice, nous avons fait des progrès considérables dans le domaine de l'apprentissage organisationnel, en élaborant notamment une stratégie d'apprentissage en collaboration avec l'École de la fonction publique du Canada (EFPC), des séances d'information et de formation sur la dotation en personnel fondées sur les valeurs, des séances de formation linguistique, des évaluations de rendement pour les gestionnaires et les employés et une politique sur le harcèlement en milieu de travail. L'élaboration et la mise en œuvre d'une stratégie d'apprentissage et d'un programme éducatif en collaboration avec l'EFPC permettront au personnel de continuer à développer son expertise et les compétences requises pour accomplir ses tâches, et l'amènera à assumer de nouvelles fonctions et responsabilités.

Nous avons continué à travailler en collaboration avec des organismes centraux tels que l'Agence de gestion des ressources humaines de la fonction publique du Canada et la Commission de la fonction publique du Canada sur des mesures de suivi, conformément aux recommandations de la Commission de la fonction publique et au rapport de la vérificatrice générale du Canada en 2003. Certaines de ces mesures donneront au Commissariat la possibilité de reprendre ses pleins pouvoirs de délégation en matière de dotation.

## Finances et administration

Le Bureau du vérificateur général a émis une opinion favorable à la suite de la vérification des états financiers du Commissariat pour l'exercice 2003-2004. Voilà un jalon important et un indicateur que l'organisme a effectivement progressé dans son cheminement vers le renouvellement institutionnel. Notre organisme a profité de ce succès en mettant au point des cycles d'examen et de planification, de même qu'en simplifiant et en améliorant les pratiques de gestion financière.

## Vers le renouvellement institutionnel

La priorité numéro un de la commission a été de diriger le renouvellement institutionnel du Commissariat en renforçant les processus de gestion du CPVP, en particulier la gestion des ressources humaines et la gestion financière – planification, budgétisation, établissement de rapports et mécanismes de contrôle.

Le cadre financier global du Commissariat suit l'exercice du gouvernement (2004-2005).

### La planification et l'établissement de rapports

Un élément de base du renouvellement institutionnel du Commissariat est la mise en place d'un processus stratégique de planification, d'établissement de rapports et de contrôle. En 2004-2005, nous avons conclu une première année sous ce processus révisé. Le plan stratégique élaboré en début d'exercice nous a servi de feuille de route tout au long de l'année. Les possibilités en matière d'examen et d'établissement de rapports faisaient partie de ce nouveau processus. Nous avons ajusté les plans et les budgets tout au long de l'année. Pour nous aider à établir des rapports et à procéder à des examens, nous avons mis sur pied un cadre de mesure du rendement et un rapport mensuel sur le rendement. Nous avons également initié une révision des processus pour l'ensemble de l'organisme, ce qui permettra au Commissariat de déterminer avec plus de justesse les besoins en ressources et de rédiger une analyse de rentabilisation pour le financement permanent.

### Les ressources humaines

Nous continuons à travailler à l'élaboration et à la mise en œuvre de changements en vue d'améliorer la façon dont le Commissariat est géré et la qualité du milieu de travail. Des changements considérables et des améliorations ont été apportés aux pratiques et aux politiques de gestion des ressources humaines.

Au cours de la prochaine année, le Commissariat continuera à prendre en charge les activités ci-haut mentionnées. Nous espérons également être en mesure d'entreprendre davantage d'activités de sensibilisation du grand public plus proactives dans notre stratégie en matière de communications et d'information.



téléchargeable de la commissaire sur la conformité à la *LPRPDE*. Il nous fait plaisir de signaler que depuis 2001, le nombre de visites de notre site a plus que quadruplé, atteignant 922 106 en 2004.

## Publications

Le Commissariat a produit des documents d'information, dont des guides sur la *LPRPDE* à l'intention des personnes, des organisations et des entreprises, ainsi que de nouvelles fiches d'information traitant de sujets tels que le consentement, l'utilisation du numéro d'assurance sociale dans le secteur privé, la circulation transfrontalière des renseignements personnels et la façon dont le Commissariat mène des enquêtes sur de possibles violations de la vie privée.

En 2004-2005, en plus de préparer de nouvelles fiches d'information, nous avons élaboré une trousse d'information électronique à l'intention des entreprises pour aider celles-ci à se conformer à la nouvelle loi. Nous avons révisé la teneur de nos guides afin de nous assurer que ceux-ci étaient à jour pour la mise en œuvre intégrale de la *LPRPDE* le 1<sup>er</sup> janvier 2004. Nous avons reçu tous les jours des demandes au sujet de ces documents. Ceux-ci étaient acheminés aux personnes qui en faisaient la demande ou distribués lors de conférences et événements spéciaux, et les visiteurs de notre site Web pouvaient également les obtenir en format électronique. En 2004, près de 22 000 publications du Commissariat (guides, fiches d'information, rapports annuels, copies des deux lois fédérales sur la de protection des renseignements personnels) ont été distribuées, sans compter les 742 000 publications téléchargées de notre site Web.

## Communications internes

Le Commissariat a également mis l'accent sur les activités de communications internes, qui ont joué un rôle majeur en 2004 en favorisant une plus grande transparence entre le personnel et la direction, en particulier pendant le renouvellement institutionnel en cours, mais aussi lors des activités quotidiennes. Les activités de communications internes en 2004 consistaient à fournir au personnel des renseignements, notamment sur des questions en matière de ressources humaines, les discours à venir, les présentations devant le Parlement, les réunions des comités de la haute direction et de consultation patronale-syndicale et des activités spéciales telles que des réunions de l'ensemble du personnel et des séances d'information. Le Commissariat travaille actuellement à la mise sur pied d'un réseau intranet, un portail de communications internes qui accueillera toutes les communications internes et maximisera l'accès à l'information pour le personnel. Le réseau sera lancé en 2005.

**Discours et événements spéciaux**

Les discours ont aidé le Commissariat à sensibiliser les divers auditoires et autres milieux aux enjeux relatifs à la protection de la vie privée, notamment des associations professionnelles et d'industries, des organismes sans but lucratif, des groupes de défense et des universités. En 2004, la commissaire, les commissaires adjoints et les autres représentants ont présenté plus de 19 discours portant sur des enjeux ayant des répercussions sur la protection des renseignements personnels tels que des initiatives en matière de sécurité et la prestation de soins de santé.

En mars 2004, le Commissariat a commencé à présenter une série de conférences internes (en moyenne une par mois). Lors de ces séances d'information, des experts invités ont abordé diverses questions portant sur la protection des renseignements personnels devant des membres du milieu de la protection de la vie privée et devant le personnel du CPVP. En 2004, le Commissariat a présenté dix de ces séances d'information.

### **Relations avec les médias**

En 2004, les médias ont continué à porter un intérêt soutenu sur la protection de la vie privée couvrant abondamment des questions telles l'entrée en vigueur de l'ensemble des dispositions de la *LPRPDE*, comme le témoignent de nombreux appels médiatiques au CPVP et des entrevues accordées par ce dernier. De plus, grâce à d'autres efforts proactifs en matière de relations médiatiques, tels que la diffusion de communiqués de presse, le Commissariat a eu l'occasion d'entreprendre des activités de sensibilisation, notamment pour le lancement de son programme des contributions, pour faire connaître le point de vue de la commissaire sur d'importantes lois telle la *Loi sur la sécurité publique* et sur le projet de loi visant à créer une liste nationale des abonnés auto-exclus, et pour communiquer le point de vue du Commissariat sur la circulation transfrontalière des renseignements personnels.

### **Site Web**

Nous affichons de façon continue sur notre site Web des renseignements nouveaux et pertinents. Des fiches d'information, communiqués, discours, résumés de conclusions d'enquêtes en vertu de la *LPRPDE* sont affichés sur le site afin de maintenir l'intérêt des personnes et des organisations. En 2004-2005, le Commissariat a restructuré son site Web afin qu'il soit conforme à la normalisation des sites Internet telle qu'elle a été établie par le Conseil du Trésor. Résultat : la conception et les outils de navigation du site ont été améliorés en vue de faciliter la consultation du site. Le Commissariat a également rendu le site plus interactif en y intégrant un discours

# Sensibilisation du grand public et communications

Le Commissariat à la protection de la vie privée du Canada est chargé, en vertu de la *LPRPDE*, d'élaborer et d'entreprendre des programmes d'information afin que le public et les organisations comprennent et reconnaissent d'avantage les règles qui régissent la collecte, l'utilisation et la communication des renseignements personnels. Bien qu'aucun mandat législatif de sensibilisation du grand public ne soit spécifié aux termes de la *Loi sur la protection des renseignements personnels*, le Commissariat a bel et bien le mandat de s'assurer que les ministères et organismes sont tenus responsables de leurs pratiques en matière de traitement des renseignements personnels. Il s'avère souvent nécessaire d'informer le public, ainsi que les ministères et les organismes, des exigences de la Loi et des politiques connexes ainsi que des répercussions des initiatives du gouvernement, courantes ou proposées, sur le droit à la vie privée des Canadiennes et des Canadiens.

En 2004, le Commissariat a entrepris un projet de planification stratégique des communications avec l'expertise de consultants externes ; cela a donné lieu à une stratégie exhaustive en matière de communications et d'information pour les prochains exercices. Cette stratégie permettra au Commissariat d'adopter une approche plus globale et plus proactive de la planification et de la prestation des activités de communications, une approche des communications se rapportant à la *LPRPDE* d'avantage axée sur la sensibilisation du grand public afin de mieux faire connaître le Commissariat et les principaux enjeux en matière de protection de la vie privée conformément aux deux lois.

En plus de l'élaboration de cette stratégie, le Commissariat a entrepris les activités de communications suivantes en 2004 :

**3web Corporation c. Llano Gorman et la commissaire à la protection de la vie privée du Canada**

N° de dossier de la Cour fédérale T-1603-04

M. Gorman s'est plaint que 3web Corporation, un fournisseur de services Internet qui a été son employeur, avait installé des caméras Web pour surveiller ses employés sur les lieux de travail. Ces caméras se trouvaient au service de la vente et du marketing et dans la section du personnel de soutien technique. La commissaire a conclu que la plainte était fondée. Pour ce faire, elle a déclaré ce qui suit : a) il est improbable qu'une personne raisonnable considère que le productivité des employés constitue une raison appropriée pour recourir à la surveillance vidéo et audio ; b) en utilisant des caméras Web de la manière décrite dans cette plainte, l'entreprise ne reconnaissait pas le droit fondamental de ses employés à la vie privée ; l'équilibre à laquelle fait référence l'article 3 de la *LPRPDE* s'éloigne beaucoup trop de la protection de la vie privée des personnes. L'utilisation de caméras à ces fins met en péril la *LPRPDE*.

La *LPRPDE* permet à un plaignant ou à la commissaire à la protection de la vie privée de demander à la Cour fédérale la tenue d'une audience sur toute question dont traite le rapport de la commissaire. Si le rapport de la commissaire contient uniquement des recommandations, il n'existe aucune disposition du genre pour une organisation défenderesse. Dans la présente affaire, l'organisation a formulé une demande de contrôle judiciaire. L'entreprise a nommé M. Gorman à titre d'intimé, bien qu'elle ait aussi sollicité une ordonnance pour que le rapport de la commissaire adjointe à la protection de la vie privée soit déclaré « illégal et invalide ».

En octobre 2004, la commissaire à la protection de la vie privée a déposé une requête afin de demander a) qu'elle soit ajoutée à titre d'intervenante et b) que la demande de contrôle judiciaire soit radiée. Cette requête a été entendue en février 2005, date à laquelle la commissaire a été ajoutée en qualité d'intervenante aux procédures. La Cour a rejeté la requête de la commissaire qui demandait que soit radiée la requête dans son ensemble et a conclu qu'il valait mieux la soumettre à l'instruction.

L'entreprise a abandonné les procédures en juin 2005.



## Contrôle judiciaire

Les cas suivants revêtent une importance particulière au moment de définir l'ampleur des pouvoirs d'application de la loi que confère la *LPRPDE* à la commissaire :

### ***Blood Tribe Department of Health c. commissaire à la vie privée du Canada et al.***

N° de dossier de la Cour fédérale T-2222-03 et n° de dossier de la Cour d'appel fédérale A-147-05

Une plainte a été déposée auprès du Commissariat à la protection de la vie privée alléguant (entre autres choses) que le *Blood Tribe Department of Health* avait refusé à une personne l'accès à ses renseignements personnels sans justifier son refus.

Nous sommes d'avis que la commissaire doit avoir accès à tous les documents pour s'assurer que les exceptions invoquées ont été bien appliquées et pour éviter les abus. Toutefois, le *Blood Tribe Department of Health* a refusé de donner à la commissaire accès à des documents protégés par le secret professionnel. En raison de ce refus, le Commissariat a pris sa première ordonnance de production de dossiers conformément aux alinéas 12(1)a) et c) de la *LPRPDE*.

En réponse, le *Blood Tribe Department of Health* a déposé, conformément à l'article 18.1 de la *Loi sur les cours fédérales*, une demande de contrôle judiciaire de la décision de la commissaire à la protection de la vie privée de prendre une ordonnance de production de dossiers. La Cour a rejeté cette requête en mars 2005. Le juge Mosley a déclaré que lorsque la commissaire à la protection de la vie privée est saisie d'une plainte au sujet de la conservation et de l'utilisation de renseignements personnels, il lui incombe de déterminer les faits et de rédiger un rapport présentant ses conclusions. Elle ne peut pas réaliser cette tâche si on lui refuse l'accès aux renseignements nécessaires pour vérifier les faits simplement parce qu'une revendication de privilège de non-communication est formulée. La Cour était convaincue que la commissaire à la protection de la vie privée avait correctement exercé son pouvoir de prendre une ordonnance de production de dossiers. Cette ordonnance ne limite ni ne refuse le droit au secret professionnel dont peut jouir le demandeur concernant les documents en question.

Le demandeur a déposé une demande d'appel relativement à cette décision en avril 2005.



que ces communications ont causé beaucoup de tort à sa réputation et ont contribué à sa décision de démissionner de la direction de son entreprise.

Dans ses conclusions, la commissaire adjointe a reconnu que la *LPRPDÉ* permet à une organisation de communiquer les renseignements personnels concernant une personne sans le consentement de cette dernière dans le but de recouvrer une créance. Toutefois, cette exception ne donne pas *carte blanche* à une organisation pour communiquer tous les renseignements qu'elle souhaiterait. La commissaire adjointe est d'avis que dans la situation en cause, il était clair qu'une quantité excessive de renseignements personnels avait été communiqués. Par conséquent, elle a déterminé que la banque se trouvait en infraction relativement au principe 4.3 de l'annexe 1 de la *LPRPDÉ* et elle a conclu que la plainte était fondée.

Une requête a été déposée devant la Cour fédérale le 1<sup>er</sup> décembre 2004. On s'attendait à ce que la commissaire à la protection de la vie privée demande l'autorisation de se présenter devant la Cour, conformément à l'alinéa 15(7) de la *LPRPDÉ*. Toutefois, un règlement a été conclu lors de la conférence de règlement des litiges tenue avant le procès et, par conséquent, la requête a été rejetée le 15 juin 2005.

**Richard Breithaupt et Peggy Fournier c. Halli MacFarlane et Calm Air International Ltd.**  
N° de dossier de la Cour fédérale T-2061-04

M. Breithaupt s'est plaint qu'une employée de Calm Air (M<sup>me</sup> MacFarlane) a communiqué à la GRC des renseignements sur son itinéraire et celui de son épouse sans leur consentement et sans les prévenir. Il a été confirmé que l'employée de Calm Air a obtenu l'accès à ces renseignements sans que les intéressés n'en soient informés ni aient donné leur consentement. Toutefois, l'employé en question de Calm Air et l'agent de la GRC ont tous deux nié le fait que cet employé ait communiqué ces renseignements à un agent de la GRC.

Les éléments de preuve documentaire ont incité la commissaire adjointe à conclure qu'il y avait effectivement eu communication. Elle a constaté que l'employée avait utilisé ces renseignements à des fins autres que celles auxquelles ils avaient été colligés et les avait ensuite communiqués, contrevenant ainsi aux principes 4.3 et 4.5 de l'annexe 1 de la *LPRPDÉ*. Par conséquent, la plainte était fondée.

Le plaignant a déposé une plainte en vertu de l'article 14 de la *LPRPDÉ* devant la Cour fédérale le 18 novembre 2004. La commissaire n'est pas partie prenante de cette requête, bien qu'elle en suive le déroulement.

le droit à la vie privée des employés et les besoins de l'employeur avait été atteint. L'objectif était raisonnable et approprié et Telus avait adéquatement informé ses employés de l'objectif visé et avait pris les mesures de sécurité adéquates concernant les renseignements personnels.

Après que la commissaire adjointe à la protection de la vie privée a fait connaître ses conclusions, chacune des quatre plaintes s'est transformée en requête distincte auprès de la Cour fédérale en vertu de l'article 14 de la *LPRPDE*. Une ordonnance datée du 31 décembre 2004 consolidait ces requêtes dans un même dossier de la Cour fédérale portant le n° T-1865-04.

La commissaire à la protection de la vie privée a alors demandé, conformément à l'alinéa 15c) de la *LPRPDE*, d'être nommée partie prenante à ces requêtes afin de présenter des observations visant à aider la Cour à élaborer des critères pour évaluer l'équilibre entre les besoins commerciaux et les droits des particuliers en matière de protection de la vie privée. Telus a consenti à la requête, mais a fait des observations à la Cour selon lesquelles l'entreprise suggère de limiter le rôle de la commissaire à la protection de la vie privée. La commissaire a réussi à faire rejeter ce point de vue et a obtenu, le 22 février 2005, le statut de partie à part entière.

La commissaire a fait des observations sur plusieurs questions, dont les suivantes : 1) le syndicat des employés des télécommunications n'était pas un demandeur adéquat dans le cadre de cette audience ; 2) la Cour devrait tenir compte des facteurs à prendre en considération dans la recherche d'un équilibre entre les intérêts des parties ; 3) le cadre juridique et les facteurs utilisés par la commissaire dans la recherche de l'équilibre entre les intérêts des parties devrait être appliqué par la Cour ; 4) la *LPRPDE* n'exige pas que l'employeur demande le consentement du syndicat au lieu de demander directement le consentement des employés ; 5) les attentes en matière d'exigences quant au consentement ne s'appliquent pas dans cette situation ; 6) à quel moment la possibilité de consentement peut-elle être sous-entendue ; 7) la reconnaissance de la capacité de retirer son consentement.

Une audience est prévue pour le 20 septembre 2005.

**John Testa et Brenda Marie Testa c. Citibank**

N° de dossier de la Cour fédérale T-2135-04

M. Testa a affirmé que la Citibank avait communiqué une quantité importante de renseignements personnels à ses employés sans son consentement. Il a ensuite soutenu

des conversations ont été enregistrées, l'entreprise n'a pas réellement réussi à recueillir ou à utiliser des renseignements personnels. Il n'y a donc pas eu d'infraction à la *LPRPDE* puisqu'une tentative d'enfreindre la Loi n'est pas une infraction de la *LPRPDE*.

Quant à la question de faire preuve de réserve à l'égard de la décision de la commissaire à la protection de la vie privée, la Cour a conclu qu'elle peut se fier à la décision de la commissaire à la protection de la vie privée ou à certaines parties de celle-ci dans sa détermination, mais qu'elle n'est pas contrainte de le faire. Au moment d'exercer son pouvoir discrétionnaire *de novo*, la Cour fera preuve de moins de réserve à l'égard de la décision de la commissaire à la protection de la vie privée qu'elle ne l'aurait fait. Toutefois, on doit tenir compte des facteurs pris en considération par la commissaire à la protection de la vie privée dans l'examen des intérêts en matière de protection de la vie privée de la plaignante et l'intérêt légitime de l'employeur qui cherche à protéger ses employés et ses biens.

En avril 2005, M<sup>me</sup> Morgan a déposé une demande d'appel.

**Paul Wansink et Telecommunications Workers Union c. Telus et la commissaire à la protection de la vie privée du Canada**

N° de dossier de la Cour fédérale T-1862-04

**Henry Fenske et Telecommunications Workers Union c. Telus et la commissaire à la protection de la vie privée du Canada**

N° de dossier de la Cour fédérale T-1863-04

**Paul Bernat et Telecommunications Workers Union c. Telus et la commissaire à la protection de la vie privée du Canada**

N° de dossier de la Cour fédérale T-1864-04

**Randy Turner et Telecommunications Workers Union c. Telus et la commissaire à la protection de la vie privée du Canada**

N° de dossier de la Cour fédérale T-2222-03

Les demandeurs se sont plaints auprès de la commissaire à la protection de la vie privée que leur employeur, Telus Communications Inc., ait enfreint la *LPRPDE* en les obligeant à consentir à la collecte de données biométriques les concernant et à fournir les renseignements qui permettraient à un ordinateur d'authentifier automatiquement leur identité à partir de leur empreinte vocale.

La commissaire adjointe à la protection de la vie privée a évalué l'exigence visant l'empreinte vocale et a déterminé qu'il ne s'agissait pas d'une pratique qui porte gravement atteinte à la vie privée. Elle s'est dit d'avis qu'un juste équilibre entre

**Janice Morgan c. Alta Flights (Charters) Inc. et la commissaire à la protection de la vie privée du Canada**  
N° de dossier de la Cour fédérale T-1066-04 et n° de dossier de la Cour d'appel fédérale A-184-05

M<sup>me</sup> Morgan, ancienne employée d'Alta Flights, s'est plainte que son employeur ait tenté de recueillir et d'utiliser des renseignements personnels qui la concernent sans son consentement et sans l'en informer. Plus précisément, elle allègue qu'un directeur a placé un enregistreur numérique sous une table de la salle des fumeurs, mise à la disposition des employés, afin de recueillir des renseignements personnels à leur sujet. La société a reconnu que le directeur avait tenté de colliger des renseignements personnels sur les employés sans prévenir ces derniers et sans leur consentement.

L'enquête a déterminé que puisque rien ne prouvait qu'on avait eu recours à l'enregistrement, aucun élément de preuve ne pouvait étayer la requête de la plaignante selon laquelle on avait recueilli et utilisé des renseignements personnels. La commissaire adjointe à la protection de la vie privée a conclu que la société n'avait pas enfreint la *LPRPD* et que, par conséquent, la plainte était non fondée. Toutefois, elle a prévenu l'entreprise qu'il ne fallait pas interpréter ses conclusions comme une approbation de ce que le directeur avait tenté de faire.

M<sup>me</sup> Morgan a déposé une requête devant la Cour fédérale, en vertu de l'article 14 de la *LPRPD*, le 26 mai 2004. La requête originale nommait par erreur la commissaire à la protection de la vie privée à titre d'intimée. Le 14 septembre 2004, la Cour a accepté la requête de la commissaire à la protection de la vie privée visant à être radiée à titre d'intimée et ajoutée à titre de partie dans le cadre de la requête, conformément à l'alinéa 15c) de la *LPRPD*.

Au procès, la commissaire à la protection de la vie privée a présenté ses observations concernant cinq sujets : 1) la compétence de la *LPRPD* en la matière nonobstant la formulation d'une plainte pour congédiement injuste en vertu du *Code canadien du travail* relativement à la même question ; 2) la norme de contrôle judiciaire et le devoir de réserve adéquats à l'égard des conclusions de la commissaire à la protection de la vie privée ; 3) l'interprétation juste de l'alinéa 7(1)b) ; 4) le fait de savoir si une tentative de collecte constitue une collecte ; 5) le fait de savoir s'il est du ressort d'une juridiction de common law d'accorder des recours qui ne sont pas autorisés par la *LPRPD*.

La Cour a entendu la requête le 15 mars 2005. À l'instar de la commissaire adjointe à la protection de la vie privée, la Cour a conclu qu'en l'absence de toute preuve selon laquelle



La Cour a également établi que, même s'il s'agissait d'une procédure *de novo*, le commissaire avait droit à une certaine retenue compte tenu de son expertise.

Enfin, la Cour a adopté les quatre critères proposés concernant le paragraphe 5(3) en précisant que les facteurs particuliers pris en compte en l'espèce pourraient ne pas s'appliquer dans toutes les affaires. En se servant de ces critères, la Cour a conclu qu'une personne raisonnable estimerait que les fins invoquées par l'organisation pour recueillir les images par l'entremise d'une caméra vidéo numérique sont appropriées dans les circonstances et, par conséquent, la Compagnie de chemin de fer Canadien Pacifique n'a pas enfreint la *LPRPDE*.

#### Affaires devant les tribunaux

Les cas suivants présentent un intérêt particulier dans l'interprétation continue de la *LPRPDE* :

#### Keith Vanderbeke c. la Banque royale du Canada

N° de dossier de la Cour fédérale T-222-04

M. Vanderbeke avait déjà formulé une plainte quant à la manière dont la Banque royale du Canada traitait ses renseignements personnels. Dans sa plainte relative au même sujet, M. Vanderbeke a allégué que la Banque royale avait recours à des pratiques répréhensibles systématiques dans la tenue de ses dossiers et, plus particulièrement, que la banque ne conservait pas « adéquatement » les accusés de réception du renouvellement de l'hypothèque de ses clients. La banque a expliqué qu'elle ne conservait pas de copie des accusés de réception envoyés à ses clients puisque ceux-ci contiennent des renseignements qui sont disponibles dans d'autres documents. Lors de l'examen de la plainte, la commissaire adjointe à la protection de la vie privée a estimé que la *LPRPDE* accordait aux personnes le droit d'accès au contenu des renseignements personnels, mais pas nécessairement aux documents précis qui les contiennent. Par conséquent, elle a déterminé que la plainte était non fondée.

Le 29 janvier 2004, M. Vanderbeke a déposé une requête, en vertu de l'article 14 de la *LPRPDE*. La Banque royale a présenté une requête en vue de radier la demande, mais cette requête a été rejetée.

Une motion datée du 5 juillet 2004 exigeait que M. Vanderbeke verse une consignation en justice avant de procéder à sa déclaration sous serment, ce qui a entraîné un retard dans l'audience qui a été reportée au 23 février 2005. À ce jour, la commissaire n'a pas été invitée à participer à cette requête, mais suit de près le cours de cette affaire.

compagnie pour recueillir des renseignements personnels ainsi que les circonstances entourant ces objectifs. À cette fin, il a utilisé les questions suivantes : 1) est-il possible de faire la preuve que la mesure est nécessaire pour répondre à un besoin particulier ; 2) cette mesure est-elle susceptible d'être efficace pour répondre à ce besoin ; 3) l'atteinte à la vie privée est-elle proportionnelle à l'avantage qui en découlera ; 4) existe-t-il un autre moyen moins envahissant qui pourrait permettre d'atteindre le même objectif ? L'ancien commissaire a déterminé qu'une personne raisonnable ne prendrait pas en considération ces circonstances pour justifier la prise d'une mesure portant autant atteinte à la vie privée que l'installation de caméras vidéo numériques. Par conséquent, l'utilisation de ce type de surveillance vidéo par la compagnie aux fins mentionnées n'est pas appropriée et l'entreprise contrevient au paragraphe 5(3) de la *LPRPDE*.

M. Eastmond a déposé une requête à la Cour fédérale en février 2003 en vertu de l'article 14 de la *LPRPDE*. Il sollicitait une ordonnance prescrivant la confirmation des conclusions de l'ancien commissaire ainsi que différentes autres ordonnances sur le même sujet. Il demandait aussi à l'ancien commissaire d'envoyer une copie certifiée de son rapport d'enquête.

L'ancien commissaire à la protection de la vie privée s'étant opposé à donner suite à cette demande, la Cour a décidé en juin 2003 que les *Règles de la Cour fédérale* ne permettaient pas à un demandeur d'exiger des documents en la possession du commissaire à la protection de la vie privée.

Le commissaire à la protection de la vie privée par intérim a été ajouté à titre de partie en vertu de l'alinéa 15c) de la *LPRPDE*, mais ne s'est pas prononcé sur l'issue ultime de l'affaire quant au faits. Il a plutôt soutenu que la Cour devrait accorder une certaine retenue judiciaire à l'expertise du commissaire et adopter les quatre critères pour déterminer la pertinence de la collecte des renseignements par la Compagnie de chemin de fer Canadien Pacifique. Un autre mémoire a été déposé en décembre 2003 traitant de la compétence du commissaire et de la Cour en la matière, même si l'affaire découle d'une situation d'emploi visée par une convention collective. Selon le mémoire complémentaire, il y a juridiction concurrente dans cette situation.

La requête a été entendue en avril 2004. Le 11 juin 2004, la Cour a fait connaître sa décision. La Cour a conclu que le commissaire à la protection de la vie privée avait compétence en la matière, que l'essentiel du litige ne découlait pas de la convention collective et que le Parlement n'avait pas l'intention d'exclure les syndiqués du champ d'application de la *LPRPDE*.

M. Englander a déposé sa toute première requête à la Cour fédérale en vertu de l'article 14 de la *LPRPDE* après que l'ancien commissaire a fait connaître ses conclusions. Ce dernier n'était pas partie prenante à ces procédures. En bout de ligne, la Cour fédérale a conclu que M. Englander ne l'avait pas convaincu que sa requête était fondée et a rejeté celle-ci. Elle a adjugé les dépenses à l'intimé.

M. Englander a déposé un appel devant la Cour d'appel fédérale. L'actuelle commissaire à la protection de la vie privée a été autorisée à intervenir dans le cadre de cet appel.

La Cour a entendu l'appel le 7 octobre 2004. Dans sa décision, rendue le 17 novembre 2004, elle a accueilli l'appel en partie à la lumière du fait que Telus n'obtenait pas le consentement éclairé de ses nouveaux clients avant d'utiliser les renseignements personnels qui les concernent dans ses annuaires téléphoniques; il ne s'agit pas de consentement éclairé lorsque la personne censée donner ces renseignements ne sait pas au moment de le faire qu'elle peut refuser. Le fait d'informer les clients après-coup peut constituer un facteur pouvant faire l'objet d'une évaluation de la conformité conformément au principe de « transparence », mais arrive trop tard pour respecter le principe du consentement éclairé. La Cour a insisté sur le fait que, dans ce cas-ci, le consentement est crucial puisqu'il ouvre la voie à la publication des renseignements personnels.

La Cour a déclaré dans sa décision du 9 février 2005, qu'étant donné que Telus avait commencé à modifier ses pratiques pour se conformer à la *LPRPDE*, il n'était pas nécessaire d'exiger que Telus apporte les changements nécessaires. Selon le jugement : « la Cour est convaincue qu'il suffit en l'espèce de déclarer que Telus a enfreint l'article 5 de la *Loi sur la protection des renseignements personnels et les documents électroniques* et qu'il n'est pas nécessaire de prendre une injonction péremptoire. » [Traduction]

### **Erwin Eastmond c. Compagnie de chemin de fer Canadien Pacifique et Commissaire à la protection de la vie privée du Canada**

N° de dossier de la Cour fédérale T-309-03

M. Eastmond s'est plaint que son employeur recueillait des renseignements personnels sur ses employés sans leur consentement. Le plaignant était surtout préoccupé par le fait que des caméras d'enregistrement vidéo numériques installées dans la cour de la compagnie pourraient recueillir des renseignements personnels sur les employés.

L'ancien commissaire à la protection de la vie privée a invoqué le paragraphe 5(3) et expliqué qu'il devait prendre en considération la pertinence des objectifs de la

## Décisions importantes

Les demandes en vertu de la *LPRPDÉ* décrites ci-après méritent qu'on s'y arrête :

**Mathew Englander c. Telus Communications Inc. et Commissaire à la protection de la vie privée du Canada**  
 N° de dossier de la Cour fédérale T-1717-01 et n° de dossier de la Cour d'appel fédérale A-388-03

M. Englander a allégué que Telus utilisait et communiquait les nom, adresse et numéro de téléphone de ses clients dans les pages blanches de son annuaire et ailleurs, à l'insu de ses clients et sans avoir obtenu leur consentement. Il a également soutenu que Telus exigeait indûment des frais à des clients qui demandent la « non-publication » de leur numéro de téléphone. M. Englander soutient que les mesures prises par Telus sont contraires aux paragraphes 5(1) et (3) de la Loi ainsi qu'à plusieurs clauses de l'annexe 1 de la Loi.

Au sujet du consentement, l'ancien commissaire a conclu que l'entreprise avait de fait obtenu un consentement valable de manière implicite et que celle-ci s'était conformée aux règlements concernant les renseignements mis à la disposition du public. Il a accordé une attention particulière à la question que l'entreprise posait à ses clients quant à la façon dont les renseignements les concernant devaient figurer dans les pages blanches et a établi que la question implique en soi la publication éventuelle des renseignements dans des annuaires auxquels le public a accès. Puisque les renseignements publiés par la suite sur d'autres supports correspondent simplement à ceux qui sont publiés dans les pages blanches, ils sont également tenus pour des renseignements auxquels le public a accès en vertu de la Loi et il est possible de les recueillir, de les utiliser et de les communiquer sans le consentement de la personne concernée.

Au sujet des frais exigés pour la non-publication des renseignements concernant les clients, le commissaire s'est référée à l'Ordonnance Télécom 98-109 du CRTC qui stipule que les sociétés de télécommunications peuvent exiger jusqu'à 2 \$ par mois pour un service de numéro non publié. Par conséquent, il a conclu que l'entreprise en cause était habilitée à exiger son tarif mensuel de non-publication établi à 2 \$ et que cette mesure n'était pas déraisonnable.



- Keith Vanderbeke c. Banque royale du Canada (n° de dossier de la Cour fédérale T-222-04)
- Ron Gass c. NAV Canada (n° de dossier de la Cour fédérale T-821-04), rejetée en juillet 2004 (par consentement)
- Pierre Jean Trudeau c. Banque TD Canada Trust (n° de dossier de la Cour fédérale T-851-04), rejetée le 23 février 2005 (en raison du délai)
- Bradley Nazarko et Travailleurs unis des transports, section 691 c. Compagnie des chemins de fer nationaux du Canada (n° de dossier de la Cour fédérale T-948-04), abandonnée le 8 juillet 2005
- Janice Morgan c. Alta Flights (Charters) Inc. (n° de dossier de la Cour fédérale T-1066-04)
- Ian David Kosher c. Banque Canadienne Impériale de Commerce (n° de dossier de la Cour fédérale T-1143-04)
- 3web Corporation c. Llano Gorman (n° de la Cour fédérale T-1603-04), abandonnée en juin 2005
- Paul Wansink et Telecommunications Workers Union c. Telus Communications Inc. (n° de dossier de la Cour fédérale T-1862-04), jointe au n° de dossier de la Cour fédérale T-1865-04 le 31 décembre 2004
- Henry Fenske et Telecommunications Workers Union c. Telus Communications Inc. (n° de dossier de la Cour fédérale T-1863-04), jointe au n° de dossier de la Cour fédérale T-1865-04 le 31 décembre 2004
- Paul Bernat et Telecommunications Workers Union c. Telus (n° de dossier de la Cour fédérale T-1864-04), jointe au n° de dossier de la Cour fédérale T-1865-04 le 31 décembre 2004
- Randy Turner et Telecommunications Workers Union c. Telus (n° de dossier de la Cour fédérale T-1865-04)
- John Testa et Brenda Marie Testa c. Citibank (n° de dossier de la Cour fédérale T-2135-04), rejetée le 15 juin 2005 (réglement intervenu lors de la conférence préalable à l'instruction)
- Richard Breithaupt et Peggy Fournier c. Hali MacFarland et Calm Air International Ltd. (n° de dossier de la Cour fédérale T-2061-04)

## Requêtes en vertu de la LPRPDE

En vertu de l'article 14 de la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)*, une personne ayant porté plainte a le droit, à l'issue de l'enquête de la commissaire et après le dépôt de son rapport, de déposer une demande d'audience à la Cour fédérale sur toute question traitée dans ce rapport. Il doit s'agir de questions qui figurent parmi les sujets dont traite l'article 14. Ce dernier article accorde à la commissaire le droit de déposer directement une demande à la Cour fédérale à l'égard d'une plainte qu'elle a déposée de son propre chef.

En vertu de l'article 15 de la *LPRPDE*, la commissaire peut (avec le consentement du plaignant) demander directement une audience à la Cour sur toute question visée par l'article 14, comparaitre devant la Cour au nom de tout plaignant qui a présenté une demande d'audience en vertu de l'article 14, ou, avec l'autorisation de la Cour, comparaitre comme partie à une instance engagée par toute autre partie que la commissaire en vertu de l'article 14.

Du 1<sup>er</sup> janvier 2001 au 31 décembre 2004, 35 demandes ont été déposées devant la Cour fédérale au titre de la *LPRPDE*, dont quinze en 2004. Ainsi, le nombre de demandes déposées en 2004 seulement est presque égal au nombre total de demandes déposées depuis l'entrée en vigueur de la *LPRPDE* jusqu'au début de l'année 2004. Il s'agit donc d'une hausse énorme. La liste suivante contient toutes les demandes déposées devant la Cour fédérale en vertu de la *LPRPDE* en 2004 :

- Karen et Daniel Edwards c. Banque Canadienne Impériale de Commerce (n° de dossier de la Cour fédérale T-35-04), abandonnée le 2 novembre 2004



- Le cadre comprend la vérification interne des systèmes et des pratiques afin que les organisations respectent leurs obligations en matière de protection des renseignements personnels. Les outils d'autoévaluation (programme de vérification) seront aussi affichés sur notre site Web ; et l'exécution d'une enquête sur l'industrie privée concernant l'utilisation des dispositifs d'identification par radiofréquence.

## À l'affût de l'identification par radiofréquence

Nous continuons de surveiller l'évolution de la technologie des dispositifs d'identification par radiofréquence (RFID). Nous estimons que les entreprises doivent établir des politiques et des normes avant de mettre en application la technologie des dispositifs d'identification par radiofréquence, et non pas après-coup. Toute utilisation des dispositifs d'identification par radiofréquence doit être conforme aux exigences de la *LPRPDE*. De plus, nous voulons connaître le rôle des applications des dispositifs d'identification par radiofréquence en matière d'agrégation et d'exploration de données, puisque ces dernières dépendent de l'obtention d'une quantité toujours croissante de détails au sujet des personnes et de ce qu'elles achètent ou louent.

Nous prévoyons envoyer des lettres à des sociétés canadiennes sélectionnées qui seraient susceptibles de recourir aux dispositifs d'identification par radiofréquence afin de mieux comprendre le nouvel usage de ces dispositifs. Notre intérêt premier est d'apprendre comment ces dispositifs pourraient être utilisés pour établir des liens entre les renseignements personnels et les produits et services. Nous désirons savoir si cette technologie sera utilisée pour identifier ou suivre des personnes. Nous désirons également savoir si, au moment d'élaborer et de mettre en œuvre les applications liées aux dispositifs d'identification par radiofréquence, les entreprises évalueront les menaces ou les risques ou encore les conséquences sur la protection de la vie privée et comment les employés et les consommateurs seront informés de la présence de ces dispositifs.

Les résultats de cette enquête seront publiés dans le rapport annuel de l'an prochain. Nous ne communiquerons pas de renseignements commerciaux de nature exclusive. Nous continuerons de surveiller les progrès en matière de technologie des dispositifs d'identification par radiofréquence pour déterminer les sphères qui nécessiteront de l'encadrement quant aux questions de protection des renseignements personnels.



de risques en matière de protection de renseignements personnels. Les risques de données, le vol d'identité, la collecte, la conservation et l'utilisation inappropriées de renseignements personnels et le défaut d'agir en cas de manquements relatifs à la protection des renseignements personnels.

Il faudra du temps pour bâtir la capacité pour entreprendre des vérifications suffisantes et appropriées. La Direction ne compte actuellement que quatre agents de vérification en tout pour effectuer le travail dans les secteurs public et privé. La portée de l'« univers de la vérification » se compose de plus de 150 ministères et organismes fédéraux assujettis à la *Loi sur la protection des renseignements personnels* et de milliers d'organisations commerciales au Canada assujetties à la *LPRPDE*.

Les démarches que le Commissariat entreprendra pour renforcer la fonction de vérification sont notamment :

- l'achèvement de méthodes et de pratiques d'examen et de vérification externes ;
- la définition du but de la Direction et l'articulation de l'organisation autour des valeurs prônant le travail d'équipe ;
- l'amorce d'un processus visant à élaborer une stratégie et un plan de vérification à plus long terme compte tenu des risques et des enjeux relatifs à la protection des renseignements personnels ;
- l'élaboration d'une analyse de rentabilisation qui sera présentée au Conseil du Trésor du Canada afin d'obtenir davantage de financement pour la vérification et l'examen ;

- la sensibilisation auprès des comités parlementaires en ce qui touche les vérifications en matière de protection des renseignements personnels ;
- la mise sur pied d'un projet visant à déterminer et à mettre à l'essai un processus pour établir s'il y a « motifs raisonnables » pour sélectionner l'objet des vérifications menées en vertu de la *LPRPDE*. Les critères et le processus seront publiés sur notre site Web au cours du prochain exercice financier, et tous les commentaires à ce sujet seront appréciés ;

- la mise sur pied d'un projet d'élaboration d'un outil d'autoévaluation servant à aider les organisations à se conformer à la *LPRPDE* et à promouvoir les bonnes pratiques de gestion des renseignements personnels. Nous souhaitons que les organisations comprennent qu'une bonne protection des renseignements personnels constitue une saine gestion des affaires et qu'elles ont besoin d'un solide cadre de gestion en matière de protection de la vie privée. Ce

## Renforcer la fonction de vérification

Le paragraphe 18(1) de la *LPRPDE* permet à la commissaire de procéder à la vérification des pratiques de gestion des renseignements personnels d'une organisation si celle-ci des motifs raisonnables de croire que cette organisation contrevient aux principes de pratiques équitables en matière de renseignements qui sont établies dans la Loi et dans l'annexe. À ce jour, nous n'avons mené aucune vérification en vertu de la *LPRPDE*. Toutefois, compte tenu que la *LPRPDE* est à présent en vigueur dans son intégralité et que les organisations ont eu le temps de s'y conformer, le Commissariat a récemment pris des mesures pour mettre en application ses pouvoirs de vérification là où il est justifié de le faire.

En mars 2005, la Direction de l'examen de la conformité est devenue la Direction de la vérification et de la revue, ce qui témoigne d'une importante transformation. Le Commissariat entend avoir recours davantage à la vérification, qui deviendra un outil important servant à remplir notre mandat établi en vertu de la *Loi sur la protection des renseignements personnels* et de la *LPRPDE*.

L'objectif de la Direction de la vérification et de la revue est de procéder de façon objective et indépendante à la vérification et à l'examen de systèmes de gestion de renseignements personnels dans le but de promouvoir la conformité aux lois en vigueur, aux politiques et aux normes et d'améliorer les pratiques en matière de protection de la vie privée et d'imputabilité.

L'année 2004 marque le début des efforts visant à reconstruire et à renforcer les fonctions de vérification et d'examen. Les vérifications n'ont pas encore été exploitées à leur pleine capacité, ni comme un des outils clés servant à examiner le grand nombre



à accroître considérablement la conformité des organisations défendresses à la Loi. Près de la moitié des mesures satisfaisantes prises par les organisations l'ont été, non pas à la suite des recommandations dans une lettre de conclusions, mais plutôt durant l'enquête même ou comme résultat direct de celle-ci. Autrement dit, les enquêteurs du Commissariat ont été les principaux acteurs dans la résolution de problèmes et dans près de la moitié des cas de mesures satisfaisantes prises par une organisation.

Notre taux de réussite démontre non seulement l'efficacité de notre fonction d'enquête, mais aussi l'efficacité continue du rôle d'ombudsman de la commissaire. Bien que notre dossier soit déjà étoffé, nous prenons des mesures pour l'améliorer. Nous croyons que notre nouvelle procédure de suivi systématique nous permettra notamment d'assurer un taux encore plus élevé de conformité à la *LPRPDE*.



Bien qu'il ne soit pas encore achevé, le dossier regorge déjà de preuves que la plupart des organisations sous réglementation fédérale ont pris leurs responsabilités en vertu de la *LRPDE* très au sérieux. De manière générale, les organisations ont collaboré avec le Commissariat aux enquêtes sur les plaintes et ont cherché à corriger, de manière considérable et permanente, les problèmes que nous avions détectés. En outre, le dossier montre clairement que les enquêtes en elles-mêmes ont contribué

- Un programme de récompenses a non seulement amélioré ses documents de communication comme nous l'avons recommandé, mais il a apporté d'autres améliorations relatives à la protection de la vie privée allant au-delà de nos recommandations.
- En étroite collaboration avec le Commissariat, une entreprise d'études de marché a donné suite à nos recommandations concernant ses sondages auprès des consommateurs, portant notamment sur la détermination des fins et sur le consentement à la communication de renseignements à des tiers. Résultat : le formulaire et la méthode de sondage font désormais preuve de beaucoup plus de transparence et sont en conformité avec la protection de la vie privée.
- Une société de gestion de transport a intégralement mis en œuvre nos recommandations concernant sa politique de congé de maladie. Plus particulièrement, la société n'exige plus de diagnostic précis sur les certificats médicaux fournis par ses employés.
- Un transporteur aérien a considérablement amélioré sa politique et ses pratiques de protection de la vie privée liées à son programme de récompenses.
- Un radiodiffuseur a élaboré et diffusé une politique sur l'utilisation des caméras de sécurité et des contrôles d'accès.
- Dans un cas d'affichage des relevés de vente des employés, une autre entreprise de télécommunications a expliqué à ses directeurs des ventes les fins appropriées d'utilisation et de communication des renseignements personnels, a mis à jour le programme de formation de ses employés en conséquence et a révisé sa méthode de recrutement et de sélection en vue d'informer les employés des fins auxquelles les renseignements personnels recueillis par l'entreprise seront utilisés.
- Une entreprise de télécommunications a cessé d'utiliser les relevés de téléphone de ses clients pour obtenir des renseignements sur d'autres personnes.

Les mesures suivantes sont des exemples d'améliorations générales apportées par les organisations défenderesses au cours des quatre premières années de la *LPRPDf* pour donner suites à nos recommandations :

- Une banque a adopté un processus de remplacement pour accommoder les personnes qui présentent une demande de compte de dépôt et refusent de consentir à une vérification de solvabilité.
- À la suite d'une recommandation, une banque a collaboré avec les agences d'évaluation du crédit afin d'élaborer des modèles compréhensibles et conviviaux pour présenter des renseignements sur le crédit.

- Plusieurs organisations ont reconnu que l'utilisation des numéros d'assurance sociale (NAS) est une question délicate et ont modifié leurs politiques et leurs pratiques en conséquence. Une banque, par exemple, a cessé d'exiger que le consommateur dévoile son NAS aux fins d'activation de carte de crédit. Une autre banque a modifié son formulaire de demande d'emprunt pour indiquer que la communication du NAS est facultative et a insisté auprès de ses employés sur le fait que le NAS n'est pas nécessaire pour traiter les demandes d'emprunt.
- Grâce à une longue consultation avec le Commissariat, une banque dont la documentation sur la protection de la vie privée était jugée la moins conforme parmi celle de toutes les banques a grandement amélioré son libellé de consentement et ses pratiques, notamment celles portant sur l'utilisation et la communication de renseignements personnels aux fins de marketing secondaire. À notre avis, la documentation de cette banque en matière de protection de la vie privée se situe maintenant parmi les meilleures.

- Une autre banque a suivi notre recommandation pour améliorer la sécurité des ordinateurs dans ses succursales.
- Une autre banque a mis fin à sa pratique qui consistait à émettre des cartes de crédit non sollicitées et à créer des comptes de carte de crédit sans consentement.

Un établissement de prêt a mis sur pied un comité de protection de la vie privée, organisé une formation sur la protection de la vie privée et donné pour instruction à son personnel de limiter la quantité de renseignements communiqués pour recouvrer les créances.

À la fin de 2004 et au début de 2005, dans un exercice spécial visant à établir une base solide pour ce dossier, la Direction des enquêtes et des demandes de renseignements a appliqué la nouvelle procédure de suivi aux cas antérieurs dans lesquels les réponses des organisations aux recommandations ou aux engagements n'avaient pas fait l'objet d'une mesure de suivi. Plus précisément, les enquêteurs de la Direction ont assuré le suivi de plus de 50 cas importants non vérifiés, clos entre le 1<sup>er</sup> janvier 2001 et le 1<sup>er</sup> novembre 2004, et mettant en cause des organisations sous réglementation fédérale assujetties à la *LPRPDE* depuis le début (banques, entreprises de télécommunications, entreprises de transport nationales, etc.).<sup>3</sup> Les cas visés sont ceux dans lesquels le Commissariat a décelé des lacunes en matière de protection de la vie privée et pour lesquels il a prévu que les organisations prendraient des mesures correctives précises pour donner suite aux engagements pris à la suite de notre suggestion au cours de l'enquête ou aux recommandations que nous leur avons faites ultérieurement dans les lettres de conclusions<sup>4</sup>.

Grâce aux opérations quotidiennes, le Commissariat avait déjà pu constater que les organisations défendresses avaient bien collaboré aux enquêtes et donné suite aux résultats de ces suivis parallèlement aux résultats de cas déjà connus, nous avons pu voir un tableau complet, clair et statistiquement représentatif de l'effet cumulatif de nos enquêtes sur les plaintes déposées en vertu de la *LPRPDE*.

Nous avons constaté, surtout dans les cas vérifiés pour lesquels le Commissariat s'attendait à des mesures correctives, que, neuf fois sur dix, les organisations sous réglementation fédérale avaient entièrement donné suite aux recommandations que nous avions formulées à l'issue d'une enquête. Nous avons également établi que 67 p. 100 de ses mesures satisfaisantes suscitaient une amélioration générale des organisations elles-mêmes. Autrement dit, dans environ deux cas sur trois, les mesures correctives ont dépassé le simple règlement d'une préoccupation immédiate du plaignant et poussé l'organisation à modifier considérablement ses systèmes de gestion de l'information liés à la politique, aux procédures et aux pratiques de protection de la vie privée.

<sup>3</sup> L'analyse ne comprend pas les cas des entreprises soumises à la réglementation provinciale, puisque ces organisations sont assujetties à la Loi depuis moins d'un an (1<sup>er</sup> janvier 2004).

<sup>4</sup> Par souci de temps et d'efficacité, les nombreux cas courants (en grande partie résolus) de plaintes en vertu des dispositions de la Loi relatives à l'accès n'ont pas été pris en compte dans les suivis et l'analyse.

<sup>5</sup> L'analyse représente approximativement 75 p. 100 des cas applicables clos pendant la période en question.

conserver tous les reçus seulement pendant les six mois requis et les détruire ensuite de manière sécuritaire en les déchiquetant.

L'exploitant loue la station-service d'une société d'énergie. En entrevue, le directeur de district de la société a d'abord déclaré que la politique de protection de la vie privée de la société ne s'appliquait pas aux établissements loués. Il a par la suite admis que la société s'attendait généralement à ce que les détenteurs de bail adhèrent à ses politiques et à ses procédures et que la société leur offrirait habituellement des séances de formation et d'information. Cependant, ni lui ni l'exploitant de la station-service ne pouvaient se rappeler une séance d'information sur la politique de protection de la vie privée. Le directeur de district a indiqué que la société offrirait des séances d'information aux détenteurs de bail prochainement et qu'il examinerait lui-même les politiques de protection de la vie privée lors des réunions mensuelles avec les détenteurs de bail de son district.

Le Commissariat a fait deux recommandations :

- 1) que la société s'assure de mettre en place des politiques dans l'ensemble des stations-service louées et qu'elle étudie la possibilité d'inclure une obligation à cet effet dans les contrats de location ; et
- 2) que les politiques de protection de la vie privée destinées aux stations-service de la société contiennent des procédures en vue de conserver, de protéger et d'éliminer de façon appropriée tous les renseignements personnels recueillis.

## Suivi des enquêtes sur les plaintes en vertu de la LRPDE

En 2004, nous avons adopté une procédure générale de suivi systématique des enquêtes sur les plaintes en vertu de la LRPDE. La Direction des enquêtes et des demandes de renseignements surveille désormais le progrès des organisations qui donnent suite aux engagements pris durant les enquêtes sur les plaintes et aux recommandations que le Commissariat leur a faites dans ses lettres de conclusions. Nous demandons aux organisations un rapport sur leurs intentions et leur progrès dans la tenue de ces engagements et la mise en œuvre de ces recommandations. Nous leur demandons aussi de fournir des documents attestant leur mise en œuvre.

Le but du suivi est double. Premièrement, le suivi renforce et précise les attentes du Commissariat à l'égard des mesures correctives prises par les organisations en réaction aux problèmes identifiés pendant les enquêtes sur les plaintes. Deuxièmement, il constitue un dossier permanent fiable de la conformité des organisations à la LRPDE.



- 3) que les entreprises avisent les personnes touchées lorsque des renseignements médicaux les concernant sont communiqués par inadvertance en raison de l'envoi d'une télécopie à un mauvais numéro ; et
- 4) que, chaque année, les entreprises demandent à leurs employés de renouveler les accords de confidentialité ou de protection de la vie privée, mettent à jour ces accords et révisent leurs politiques de protection de la vie privée.

### Des reçus de carte de crédit dispersés par le vent

En août 2004, un quotidien rapportait que deux femmes avaient vu des reçus de carte de crédit dispersés par le vent dans leur quartier et qu'elles étaient remontées à la source, une station-service locale, où de vieux reçus avaient été jetés dans une benne à ordures.

L'exploitant de la station a reconnu qu'il avait jeté divers reçus de 2002 dans la benne, mais a prétendu qu'il ignorait les conséquences de son geste sur la protection de la vie privée. Il a dit que ces reçus se trouvaient dans des boîtes, placées au milieu de la benne et couvertes par d'autres déchets. Il soupçonnait les enfants du voisinage d'avoir grimpé dans la benne et ouvert les boîtes par curiosité, exposant ainsi les reçus aux éléments.

Il a déclaré que ce jour-là, un journaliste l'avait informé du problème et qu'il avait pris des mesures immédiates pour ramasser les reçus éparpillés, retirer de la benne ceux qui s'y trouvaient encore et les déchiqueter. Bien qu'il soutienne que lui et ses employés n'ont pu trouver qu'une quantité minimale de reçus, notre enquête a établi que les deux femmes, premiers témoins de l'incident, avaient ramassé plus tôt trois sacs et une pleine boîte de reçus aux environs de la station-service.

Les témoins ont remis les reçus qu'elles avaient ramassés à notre enquêteur. Un échantillon de 1 897 de ces documents révèle que la plupart étaient des reçus de cartes de débit ne contenant pas de renseignements personnels permettant d'identifier quelqu'un et de nombreux autres étaient des reçus de cartes de crédit échues. Néanmoins, 151 reçus de cartes de crédit comportaient des numéros de compte valides (non pérимés), 16 contenaient des numéros de compte valides et des numéros de plaque d'immatriculation écrits à la main, trois comportaient des numéros de comptes valides et des numéros de permis de conduire écrits à la main et un comportait un numéro de permis de conduire et un numéro de plaque d'immatriculation.

L'exploitant de la station-service a donné l'assurance qu'il était maintenant conscient de ses responsabilités en vertu de la Loi et qu'il avait instauré des politiques pour

Cette entreprise a maintenant entre le numéro de télécopieur exact dans la composition abrégée afin que ses employés continuent d'envoyer leurs propres formulaires en réduisant les risques de communication involontaire. L'entreprise a également un agent de la protection de la vie privée et des politiques acceptables en matière de protection des renseignements personnels.

La troisième entreprise en cause est un organisme médical qui offre des services de consultation et dont les médecins examinent et évaluent les rapports sur les patients préparés par les nouveaux médecins consultants. La seule télécopie envoyée par erreur dans ce cas était un rapport de ce type que les médecins avaient consulté. Le médecin en cause n'avait pas envoyé la télécopie lui-même et l'entreprise n'a pas été en mesure de déterminer qui avait composé le numéro. Le rapport envoyé par télécopieur contenait le nom de la patiente, son âge et son occupation, ainsi que des antécédents médicaux détaillés concernant une blessure qu'elle avait subie dans un accident d'automobile. Il contenait également des renseignements sur ses enfants.

Lorsque le couple a appelé l'entreprise pour signaler cette erreur, un employé leur a demandé de détruire le document. Avec du recul, l'entreprise s'est rendu compte que cette directive n'était pas appropriée, en ce sens que l'employé n'avait aucun moyen de confirmer la destruction du document ou de vérifier que la méthode employée pour le faire était valable. L'entreprise a convenu d'envoyer un message pour récupérer les télécopies pouvant éventuellement être envoyées au mauvais numéro. Elle a aussi pris des mesures pour que le numéro soit vérifié avant toute transmission et que tout incident soit signalé à la direction.

À la demande du Commissariat, cette entreprise a avisé la patiente touchée par cette communication de renseignements personnels, nommé un agent de la protection de la vie privée et envoyé au Commissariat des copies de sa procédure de transmission des télécopies et de sa politique de protection de la vie privée révisées.

Le Commissariat a fait les recommandations suivantes à la première et à la troisième entreprise :

- 1) que les entreprises suivent les recommandations du Commissariat concernant la transmission de télécopies, telles qu'elles sont énoncées sur la fiche d'information *Télécopieurs et renseignements personnels*;
- 2) que les entreprises prennent des mesures pour s'assurer que les télécopies sont récupérées lorsqu'une erreur de transmission est signalée ;

renseignements personnels. Il a été établi que les cinq autres provenaient de trois entreprises distinctes.

La première est une entreprise qui possède et exploite des laboratoires médicaux. La télécopie qu'elle a envoyée par erreur au couple contenait des renseignements personnels sur une personne ayant subi des examens administrés par l'entreprise. Les renseignements comprenaient le nom, l'âge, le poids, les habitudes d'usage du tabac et le numéro de patient de la personne, ainsi qu'un diagnostic et des résultats précis d'analyses médicales.

Dans sa propre enquête interne, cette entreprise n'a pas été en mesure de déterminer lequel de ses employés avait composé le mauvais numéro de téléphone, mais elle a réussi à réduire les possibilités à cinq. Ces cinq employés étaient au courant de la nature confidentielle des dossiers médicaux et de la nécessité d'en empêcher la communication et ils avaient tous signé un accord de confidentialité en prêtant serment au moment de leur embauche, mais ils n'avaient pas été tenus de renouveler ce serment depuis.

Pour les numéros de télécopieur fréquemment utilisés, cette entreprise a ajouté dans ses ordinateurs une fonction de télécopie automatique qui sert à vérifier l'exactitude des numéros entrés dans le système avant la transmission. Quant aux numéros rarement composés (lesquels ne sont pas programmés dans le système automatisé), l'entreprise a donné à ses employés des directives pour vérifier l'exactitude de la transmission. À la demande du Commissariat, l'entreprise a entrepris de revoir ses politiques et ses procédures afin de se conformer entièrement à la *Health Information Act* de l'Alberta et à la *LPRPDE*.

La deuxième source de télécopies envoyées par erreur est une entreprise d'élimination de déchets dont les employés sont tenus de passer des examens médicaux annuels. Cette entreprise a envoyé trois télécopies par erreur, dont une portant une date antérieure à l'entrée en vigueur de la *LPRPDE*. Les deux autres étaient des formulaires remplis contenant des renseignements sur la santé de deux employés qui venaient de passer leur examen annuel. Ce n'est cependant pas l'entreprise qui a envoyé les télécopies au mauvais numéro, mais plutôt les employés eux-mêmes, chacun ayant composé le même mauvais numéro. Pour des motifs de protection de la vie privée, l'entreprise demande à ses employés d'envoyer eux-mêmes les formulaires relatifs à leur état de santé.

- a placé un message d'alarme précisant « Identité perdue ou volée » sur leur dossier de crédit afin d'inciter les créanciers à demander des preuves d'identité supplémentaires ;
- a demandé à l'autre principale agence d'évaluation du crédit de placer un message semblable sur le dossier de crédit des personnes touchées qui sont entrées en contact avec elle ; et
- a offert aux personnes touchées un abonnement annuel gratuit à un service de surveillance de crédit (la plupart ont accepté cette offre).

Pour résoudre le problème de sécurité, l'agence a apporté des modifications provisoires à ses systèmes. Ces modifications semblent efficaces en ce sens que le même contrevenant a tenté d'accéder aux dossiers de crédit un seconde fois, de la même manière, et que l'accès lui a été refusé.

Depuis l'incident, il y a eu un nombre restreint de tentatives de fraude impliquant des renseignements communiqués ; dans chaque cas, les messages d'alarme ont permis d'éviter la fraude.

### **Enquête fédérale/provinciale sur une erreur de transmission de renseignements médicaux**

En juillet 2004, un article d'un quotidien a rapporté qu'un couple marié avait reçu de sources diverses des télécopies contenant des renseignements médicaux personnels. Le couple prétend en avoir bien avisé les sources, mais il a continué de recevoir des télécopies.

Le Commissariat à l'information et à la protection de la vie privée de l'Alberta a mené une première enquête sur cet incident. Le Commissariat a établi que, bien que la loi provinciale sur la protection de la vie privée s'applique à certains renseignements transmis par télécopies, il semble que ceux-ci relèvent aussi de la juridiction fédérale en vertu de la *LPRPDE*. Le Commissariat à la protection de la vie privée du Canada a donc entrepris sa propre enquête en collaboration avec le Commissariat de l'Alberta. Le couple en question administre un immeuble à appartements. Le numéro du télécopieur qu'il utilise pour la gestion de l'immeuble ressemble à celui d'un fournisseur de soins de santé, mais deux chiffres sont intervertis. Le couple a reçu dix télécopies envoyées par erreur à leur numéro.

Le Commissariat s'est penché sur sept des dix télécopies transmises par erreur (les trois autres relèvent de la province). Deux des sept télécopies ne contenaient pas de



## Incidents en vertu de la LPRPD

En plus des plaintes individuelles provenant des personnes, le Commissariat enquête sur des incidents liés à une collecte, à une utilisation ou à une communication inappropriée de renseignements personnels qui sont portés à son attention par diverses sources, y compris les médias et l'organisation en cause. Ces enquêtes permettent souvent de mettre en lumière un problème systémique ou une atteinte à la vie privée qu'il faut régler dès que possible. Habituellement, les victimes ne sont pas identifiées, et aucune plainte écrite n'a été déposée auprès du Commissariat.

L'année dernière, le Commissariat a mené six enquêtes sur des incidents, dont trois, qui présentent un intérêt particulier, sont présentées ci-dessous.

### Communication de rapports de solvabilité à un fraudeur

En mars 2004, une agence d'évaluation du crédit a déclaré dans un communiqué qu'en raison d'un bris de la sécurité, les rapports de solvabilité de quelque 1 400 consommateurs avaient été transmis à des criminels qui se faisaient passer pour des fournisseurs de crédit. Les médias se sont emparés de l'affaire.

Le personnel de la sécurité de l'agence a découvert le bris et l'a signalé à la GRC, qui a entrepris une enquête. Il semble qu'une seule personne ait commis l'infraction et que celle-ci n'ait pas été arrêtée en mai 2004.

L'agence a confirmé que 1 398 consommateurs ont été touchés, dont 1 145 en Colombie-Britannique, 163 en Ontario et 90 en Alberta.

Les renseignements consignés dans chaque rapport de solvabilité sont le nom du consommateur, son adresse, son adresse antérieure (si disponible), sa date de naissance et son historique de paiements, ainsi que les noms et les numéros de compte de ses créanciers, les éléments de dossiers publics et les activités de perception. L'agence a confirmé que l'information communiquée ne comprenait pas les numéros d'assurance sociale ni les détails des comptes de banque.

Dans le but de remédier à la situation, l'agence :

- a avisé toutes les personnes concernées par courrier recommandé ;
- les a incitées à l'appeler et à examiner le contenu de leur dossier de crédit ;



Le rapport était erroné. En réalité, le fils n'avait pas déclaré faillite, il avait plutôt présenté une proposition à ses créanciers et satisfait aux conditions plus d'une année auparavant. La société a répondu qu'elle utiliserait un rapport de solvabilité à jour pour toute demande ultérieure. La plaignante s'est montrée satisfaite d'avoir enfin reçu une réponse de la société.

Entre-temps, le fils a réussi à louer une voiture de même marque chez un autre concessionnaire automobile. Selon la plaignante, quelqu'un chez le concessionnaire « a manifestement su comment interpréter l'information sur le crédit ».

### **Des sociétés se reprennent en mains**

#### **Un établissement de prêt**

Une femme s'est plainte qu'un établissement de crédit avait communiqué des renseignements sur son compte en souffrance à son oncle, sans son consentement.

La plainte étant jugée valable, l'établissement a ajusté le compte non payé de la plaignante et il a accepté de lui envoyer une lettre lui présentant ses excuses. Au cours de l'enquête, le Commissariat a remarqué que l'organisation n'avait pas de politiques ou de pratiques de protection des renseignements personnels. Ayant donné suite à notre recommandation pressante, l'établissement a formé un comité de protection des renseignements personnels, instauré un programme de formation pour les employés et rappelé au personnel de limiter la quantité de renseignements communiqués en vue de recouvrer une créance.

#### **Une entreprise de camionnage**

Un ancien employé prétend qu'une petite entreprise familiale de camionnage interprovincial a communiqué des renseignements personnels le concernant à un créancier sans son consentement.

Le plaignant n'avait pas de preuve pour appuyer cette affirmation et il s'est avéré que le plaignant avait lui-même fourni des renseignements au créancier. Néanmoins, notre enquête a eu pour effet de sensibiliser l'entreprise à ses obligations aux termes de la Loi. L'entreprise a instauré par la suite une politique de protection de la vie privée, nommé un agent de la protection de la vie privée, révisé ses pratiques en matière de renseignements personnels des employés et pris des mesures pour offrir à ses employés une formation sur le traitement adéquat de l'information.

## **NAS visible : une fenêtre d'enveloppe révèle trop de renseignements**

Un administrateur d'une caisse de retraite se plaint de recevoir régulièrement d'une banque des documents de transfert dans des enveloppes dont la fenêtre laisse voir le numéro d'assurance sociale (NAS) des clients. Ayan admis volontiers le problème, la banque a instauré un nouveau processus au moyen duquel le NAS et le numéro de compte ont été retirés de la partie du document réservée au nom et à l'adresse pour être placé dans une partie non visible de la fenêtre de l'enveloppe.

## **Une agence de recouvrement corrige des renseignements erronés**

Un plaignant a eu de la difficulté à obtenir du crédit parce qu'une agence de recouvrement possédait des renseignements erronés. Il avait remboursé une dette depuis plusieurs années, mais l'agence n'avait pas signalé ce fait aux bureaux de crédit. Après plusieurs tentatives infructueuses de son avocat pour faire corriger l'erreur, le plaignant s'est adressé au Commissariat.

L'agence de recouvrement n'avait aucune lettre de l'avocat dans ses classeurs. Toutefois, après avoir reçu un avis du Commissariat et une autre lettre de l'avocat, elle s'est penchée sur le dossier du plaignant, a confirmé que la dette avait été remboursée et en a informé les bureaux de crédit, lesquels ont modifié le dossier de crédit du plaignant en conséquence.

## **Un concessionnaire automobile refuse une demande de crédit sur la foi de renseignements erronés**

Une plaignante savait que sa cote de solvabilité était bonne. Quand un concessionnaire automobile a refusé la demande de crédit qu'elle et son fils avaient signée, elle a écrit à la société pour demander les renseignements sur lesquels la décision était fondée. Deux mois plus tard, elle a écrit de nouveau. N'ayant toujours pas de réponse après trois mois, elle a déposé une plainte.

Il s'est avéré que la décision était fondée non pas sur sa cote de solvabilité, mais sur celle de son fils. La société n'avait pas répondu à ses demandes d'accès à l'information parce qu'elle ne savait pas comment le faire sans dévoiler les renseignements personnels du fils. Nous avons suggéré à la plaignante d'écrire à la société une autre lettre signée par elle-même et son fils et déclarant qu'ils consentaient à la communication de renseignements personnels de l'un et l'autre. La société a finalement répondu que la demande de crédit avait été refusée en raison d'une faillite mentionnée dans le rapport de solvabilité du fils. La plaignante a de nouveau écrit à la société pour signaler que

## Communication de renseignements au syndicat sans consentement

Plusieurs employés d'une entreprise de transport se sont plaints de l'envoi au syndicat d'une liste des participants au programme de départ volontaire à leur insu et sans leur consentement. Cette liste contenait les numéros d'assurance sociale (NAS) des employés.

Ayant admis son erreur, l'entreprise a modifié le formulaire de demande concernant les indemnités de départ de manière à supprimer l'obligation d'inscrire le NAS et a ajouté un énoncé demandant à l'employé s'il consent à ce que des renseignements personnels le concernant soient communiqués au syndicat.

## Deux cas d'enveloppes interverties

Dans un cas, une plaignante a reçu de sa banque un avis relatif à un prêt étudiant, non pas le sien, mais celui de quelqu'un autre. Elle a craint que l'autre étudiant n'ait en sa possession les mêmes renseignements personnels qu'elle avait reçus à son sujet, soit son nom, son adresse, son numéro d'assurance sociale, ainsi que le numéro et le montant de son emprunt. La méprise est attribuable à une simple erreur humaine survenue en insérant les avis dans les enveloppes. Aucune autre personne du groupe d'envoi postal de la plaignante n'a reçu un avis erroné et l'étudiant dont elle avait reçu les renseignements personnels n'a pas reçu les siens, puisqu'il avait déménagé sans laisser d'adresse. La banque est parvenue à un règlement avec la plaignante et a recommandé à son personnel du centre étudiant d'être plus vigilant en préparant les documents expédiés par la poste aux clients.

Dans l'autre cas, un plaignant a reçu par la poste le billet d'avion d'une autre personne et celle-ci a reçu le billet du plaignant. Les billets contenaient des renseignements personnels sous forme d'itinéraire de voyage, d'adresse du domicile et de numéro de téléphone. Cette méprise est aussi attribuable à une erreur humaine, en ce sens qu'un employé du transporteur aérien a malencontreusement interverti les billets et les enveloppes pour les deux billets achetés par téléphone. Le transporteur aérien a présenté des excuses au plaignant et est parvenu à un règlement avec lui. Il a aussi rappelé à son employé la nécessité d'exercer une diligence raisonnable dans l'envoi de documents aux clients.

le transporteur aérien a résolu les problèmes à la satisfaction du plaignant, notamment en abandonnant la pratique des annonces d'anniversaire et en prenant des mesures pour protéger les documents contenant des renseignements personnels sur les employés et en limiter l'accès. Le transporteur a également organisé des séances d'information sur la protection de la vie privée avec la direction et le personnel administratif et a affiché un avis sur la protection de la vie privée sur un babillard interne accessible à l'ensemble des employés.

### **Un grand magasin néglige de s'identifier comme source d'un envoi postal**

Deux personnes se sont plaintes d'avoir reçu par la poste une sollicitation qui semblait provenir d'une société de surveillance du crédit. Bien qu'il semble avoir été expédié par la société de surveillance de crédit, l'envoi postal mentionnait une association avec un magasin à succursales multiples où les deux plaignants avaient un compte. Ils ont tous les deux présumé que le magasin avait communiqué leurs renseignements personnels à la société de surveillance de crédit sans leur consentement. L'un des deux plaignants avait expressément demandé au magasin de ne pas utiliser les renseignements personnels le concernant à des fins autres que celle de communiquer directement avec lui.

Dans les faits, le magasin n'avait pas communiqué les renseignements personnels à la société. Il avait plutôt préparé et expédié lui-même le publipostage, mais sous le nom d'une autre société. La politique du magasin est de recourir à l'option de refuser la communication des renseignements personnels de ses clients aux sociétés affiliées fabriquant des produits de sa propre « marque », mais le magasin ne les communique pas à des tiers non affiliés comme la société de surveillance de crédit. Dans le cas du plaignant qui avait antérieurement retiré son consentement, le magasin explique qu'il a reçu la sollicitation en raison d'un délai administratif normal dans le traitement de sa demande d'exercer l'option de retrait.

Le magasin admet cependant que l'information contenue dans sa publicité n'était pas précise et qu'il aurait dû indiquer clairement qu'il agissait au nom d'une autre société. Il a également présenté des excuses aux plaignants; il a accepté de réviser sa politique de demande de compte pour offrir aux nouveaux clients une option de refus au moment de l'ouverture d'un compte. Il a aussi entrepris de réviser les mécanismes de retrait de consentement pour assurer la cohérence de la procédure d'option de retrait dans toutes ses filiales.



Le seul document mentionnant le retrait du consentement du plaignant a été rédigé quelque temps après la communication présumée. Après avoir enregistré le retrait du consentement, la pharmacie a effectivement refusé de remplir les ordonnances du plaignant en lui expliquant qu'il s'agissait d'une pratique de la société de ne pas remplir les ordonnances des personnes ayant retiré leur consentement à la collecte, à l'utilisation ou à la communication de renseignements personnels ayant trait à leurs soins de santé. Toutefois, la documentation sur la protection des renseignements personnels de la société explique cette pratique seulement de façon générale, indiquant que le retrait du consentement peut nuire au « service ». La société a accepté de modifier sa politique en matière de protection des renseignements personnels pour préciser que les ordonnances ne sont remplies que si le consentement est donné.

### **Une compagnie d'assurance accueille les suggestions d'une plaignante au sujet du formulaire de consentement**

Une personne ayant rempli une demande d'assurance-vie s'est plainte que la compagnie d'assurance exigeait son consentement à des pratiques de collecte, d'utilisation et de communication trop générales.

Le Commissariat a organisé une téléconférence avec la plaignante et la compagnie. La compagnie lui a expliqué ses pratiques courantes, lesquelles sont conformes à la Loi. Bien que la plaignante soit satisfaite des explications, la compagnie reconnaît que la plaignante a soulevé de nombreuses questions importantes au sujet de la précision et de la clarté du libellé du consentement, lesquelles sont prises en compte dans un examen en cours. La compagnie a convenu d'envoyer à la plaignante une copie de son formulaire révisé et l'a invitée à formuler ses commentaires en vue des examens subséquents.

### **Une annonce d'anniversaire non appréciée**

Un employé d'un bureau canadien d'un transporteur aérien étranger a porté plainte quand une secrétaire a envoyé par courriel sa date de naissance à ses collègues, bien qu'il se soit déjà objecté à cette tradition locale d'annonce d'anniversaire. Il prétend également que le transporteur aérien a inscrit son adresse et son numéro de téléphone sur les listes fournies aux employés, lesquels n'ont pas besoin de connaître ces renseignements, et que ces listes ne sont pas suffisamment protégées.

À la suggestion du Commissariat, les représentants du transporteur aérien ont rencontré le plaignant pour régler les questions qu'il avait soulevées. En fin de compte,

préposé a écrit son nom et le numéro de son permis de conduire sur le billet même, expliquant que c'était une pratique de l'entreprise en raison du nombre élevé d'incidents impliquant de faux billets. Après réflexion, suite à cet incident, le plaignant craignait que ses renseignements personnels ne fussent ainsi mis à la disposition de quiconque manipulerait le billet, et ce, aussi longtemps que le billet serait en circulation.

L'entreprise a effectivement pour politique de demander au personnel de la station service de noter l'identité des clients qui présentent des billets de 100 \$, mais elle stipule que les renseignements doivent être inscrits sur des feuilles de suivi séparées, non sur les billets eux-mêmes. Bien que le préposé ait connu la procédure exacte et n'ait pas admis avoir écrit sur le billet, l'entreprise a assumé la responsabilité dans cette affaire, a présenté des excuses au plaignant et a négocié un règlement avec lui. Elle a aussi rappelé à tous ses employés de station service les procédures requises pour le traitement des renseignements personnels.

### **Une pharmacie simplifie sa procédure de consentement**

Un plaignant contestait le fait qu'une pharmacie ait exigé qu'il signe un formulaire de consentement avant de lui remettre ses médicaments. À son avis, le formulaire autorisait des pratiques de communication beaucoup trop vastes et il s'inquiétait du fait que ses renseignements personnels puissent être communiqués à des fins de marketing. Il craignait aussi de ne pas obtenir les médicaments dont il a régulièrement besoin s'il refusait de signer.

En fait, la pharmacie a succursales multiples ne communiquant pas les renseignements personnels sur ses clients à d'autres organisations à des fins de marketing. Néanmoins, en réponse aux nombreuses plaintes relatives au formulaire de consentement dont celle-ci, la société a décidé de modifier le libellé du formulaire pour le rendre plus simple et plus facile à comprendre. Elle a en outre instauré une politique et une pratique nouvelles pour les clients qui hésitent à signer le formulaire de consentement. Les clients peuvent indiquer de vive voix s'ils acceptent les pratiques de l'entreprise en matière de protection des renseignements personnels qui leur ont été expliquées par le pharmacien.

### **Une autre pharmacie clarifie sa politique de consentement**

Un client prétend que, même après qu'il a retiré son consentement aux pratiques de collecte, d'utilisation et de communication, sa pharmacie a communiqué des renseignements personnels le concernant à son médecin. Il se plaint également que la pharmacie refuse de remplir ses ordonnances parce qu'il a retiré son consentement.

évoquée, l'entreprise a fait remarquer au plaignant que plusieurs options de paiement sont accessibles aux clients et que, même si les numéros de cartes de crédit ne sont pas répétés, les clients qui choisissent de payer leurs factures par téléphone cellulaire prennent toujours le risque que les chiffres entrés au clavier soient interceptés.

#### **Une compagnie d'assurance ne tient pas compte des mises en garde d'un client**

À deux occasions distinctes, un plaignant a prévenu sa compagnie d'assurance que des personnes non autorisées pourraient essayer d'obtenir des renseignements sur les polices d'assurance qu'il détenait relativement à ses neveux. Malgré ses mises en garde et malgré les procédures d'authentification et de balisage en place à ce moment, l'information a été communiquée ultérieurement à une partie non autorisée contrairement à la volonté exprimée par le plaignant.

Le plaignant et la compagnie sont parvenus à un règlement. À la suite de la plainte, la compagnie a considérablement amélioré sa politique et ses procédures d'authentification et de balisage, et elle a intégré une nouvelle politique à la formation des représentants de son service à la clientèle.

#### **Une entreprise de transport élimine les renseignements superflus de sa base de données**

Un employé d'une entreprise de transport nationale s'est plaint du manque de sécurité des renseignements personnels dans le système automatisé de gestion du personnel. Il s'inquiétait surtout du fait que des employés non autorisés, en particulier des représentants syndicaux, pouvaient avoir accès aux renseignements personnels des employés comme leur date de naissance, leur numéro d'assurance sociale, leur taux de rémunération et leurs droits aux vacances.

Dans les faits, les représentants syndicaux n'avaient pas accès à certains des renseignements comme le craignait le plaignant. De plus, au moment de la plainte, l'entreprise avait déjà convenu que la date de naissance et le numéro d'assurance sociale étaient des renseignements personnels et procédait à l'ajustement de son système de gestion du personnel en conséquence. Enfin, l'entreprise a convenu d'enlever également du système les renseignements personnels concernant la santé.

#### **Renseignements personnels en circulation sur un billet de cent dollars**

Lorsqu'un plaignant a offert un billet de 100 \$ pour payer un achat d'essence, le préposé de la station service lui a demandé de s'identifier. D'après le plaignant, le

L'entreprise a révisé ses pratiques et convenu qu'il n'était pas nécessaire de reproduire automatiquement dans ses réponses électroniques les renseignements personnels exigés pour donner accès au site protégé. Elle a maintenant cessé d'inclure des fils de message dans ses réponses électroniques aux clients. Quant à la première préoccupation

avoir accès au courriel.

personnels sensibles soient également à la disposition de personnes qui pourraient d'information sur les comptes. Le plaignant craint à présent que ces renseignements d'identification personnelle qu'il avait eutres pour avoir accès au système sécurisé la réponse électronique de l'entreprise contenait le numéro de compte et le numéro obtienne ces numéros. Quand il a envoyé un courriel pour exprimer sa préoccupation, craignait que quelqu'un intercepte l'appel fait à partir d'un téléphone cellulaire et la date d'expiration que le client a eutres à l'aide du clavier du téléphone. Un client d'une entreprise de télécommunications, le système répète le numéro de carte de crédit Lorsque les clients paient leurs factures à l'aide du système de réponse vocale interactif

#### autre

#### Procédures concernant le téléphone et le courriel : une préoccupation de sécurité en amène une

vend.

les renseignements personnels contenus dans d'autres appareils électroniques qu'elle convient également de mettre en oeuvre des procédures semblables pour protéger à ses magasins au Canada et ils sont tenus de documenter cette mesure. L'entreprise les renseignements personnels contenus sur le disque dur des ordinateurs retournés les employés doivent dorénavant veiller à ce que soient effacés complètement tous en matière de protection des renseignements personnels et ses pratiques. Notamment, le rendre à la plaignante. L'entreprise a aussi amélioré considérablement sa politique remis en vente sans en examiner le contenu. Le magasin a pu récupérer l'ordinateur et Il s'est avéré que le magasin a réparé l'ordinateur de la plaignante et qu'un employé l'a

la concernant.

qu'il vient d'acheter un ordinateur portatif contenant des renseignements personnels s'étonne de recevoir un appel téléphonique d'un parfait étranger, lequel lui apprend le magasin d'informaticien lui en remet un neuf. Quelque temps après, la plaignante Étant dans l'impossibilité de réparer l'ordinateur d'une plaignante dans le délai prévu,

#### Un magasin prend des mesures à la suite d'un incident concernant un ordinateur portatif

Les résumés suivants sont des exemples de plaintes réglées.



d'enregistrer et des éléments probants indiquent que l'avocat avait déjà obtenu ces deux documents de ce bureau quand il a rencontré le directeur de la banque.

Cependant, pour ce qui est du relevé des opérations hypothécaires, les documents probants montrent que l'avocat avait préparé et envoyé une assignation au directeur de la banque, lui avait ensuite écrit pour obtenir un rendez-vous à la date en question et, que la veille de cette date, il avait accusé réception d'une réponse du directeur. En outre, la copie du relevé des opérations hypothécaires de la plaignante que l'avocat a présentée au tribunal a été imprimée à partir de l'ordinateur du directeur de la banque et était datée du même jour que sa réponse à l'avocat.

Le directeur n'a pas admis qu'il avait imprimé le document et l'avait fourni à l'avocat, ni qu'il avait demandé à la plaignante de ne pas révéler ses communications. Néanmoins, il a admis qu'au premier contact, il avait présumé par erreur que l'avocat agissait au nom de la plaignante.

Ayant admis que le relevé de transactions hypothécaires de la plaignante avait été communiqué à l'avocat, la banque a présenté des excuses à cette dernière.

### **Nos conclusions**

Le titre de propriété et les prêts hypothécaires grevant la propriété de la plaignante sont des renseignements accessibles au public par l'entremise du bureau d'enregistrement. De tels renseignements pouvaient donc être communiqués à l'insu et sans le consentement de l'intéressé en vertu du sous-alinéa 7(3)/1 de la Loi. Enfin, il semble que l'avocat avait déjà obtenu ces renseignements avant de s'adresser à la banque.

Il a cependant été établi que le relevé des opérations hypothécaires a été imprimé à partir de l'ordinateur du directeur de la banque le jour où ce dernier a écrit à l'avocat. Le Commissariat croit, et la banque le reconnaît, que le document a été communiqué sans le consentement de la plaignante. La plainte était fondée.

## **Choix de cas réglés en vertu de la LPPDE**

En janvier 2004, le Commissariat a la protection de la vie privée a ajouté une nouvelle catégorie de décision, « Plainte réglée en cours d'enquête ». Une plainte réglée est une plainte pour laquelle, au cours de l'enquête, le Commissariat a aidé à négocier une solution satisfaisante pour toutes les parties, y compris le Commissariat. Des 379 plaintes traitées en 2004, 152 (ou 40 p. 100) entrent dans la catégorie « réglées ».

En ce qui concerne le titre de propriété et la liste des prêts hypothécaires, notre enquête a permis d'établir que le directeur de la banque n'aurait pas eu accès à ces documents à la date en question. De plus, ces documents sont accessibles au public au bureau

ex-mari.

Dans sa plainte au Commissariat, la plaignante allègue que la banque a communiqué des renseignements personnels concernant sa situation financière à l'avocat de son

appropriées.

La plaignante croit que le directeur des services financiers de sa banque a remis ces documents et d'autres renseignements sur sa situation financière à l'avocat de son ex-mari à un certain moment. Elle dit aussi que le directeur a admis avoir agi ainsi et qu'il lui a demandé de ne pas mentionner au tribunal ses communications non

un relevé des opérations hypothécaires.

des prêts hypothécaires grevant sa maison provenant du bureau d'enregistrement et preuve par la partie adverse (son ex-mari) : le titre de propriété de sa maison, une liste sa pension alimentaire, la plaignante a reçu les copies de trois documents déposés en En assistant à une audience du tribunal concernant l'action intentée pour arriéré de

### **Les faits**

est.

suivante : quand vous avez affaire à un avocat, vérifier au départ de quel côté il Si le personnel de la banque doit tirer une leçon de cette situation, c'est la

par des traces écrites.

Dans le cas présent, heureusement, les affirmations de la plaignante sont étayées. Les cas d'affirmations divergentes peuvent être extrêmement difficiles à juger.

### **Une banque communique le dossier d'hypothèque d'une cliente à l'avocat de son ex-mari**

En somme, l'entreprise recueille et utilise des renseignements personnels au sujet des clients pour atteindre des objectifs raisonnables et ne recueille pas d'information à tort et à travers à ces fins ou à d'autres fins. La compagnie se conforme aux principes 4.4 et 4.5 ainsi qu'au paragraphe 5(3) de la Loi. La plainte était non fondée.

piratage, l'autre but de l'entreprise.

Bien que l'entreprise recueille des renseignements sur l'utilisation de la télévision à la carte grâce à la connexion téléphonique, elle le fait pour atteindre l'un de ses objectifs : facturer le client. La connexion continue est aussi un moyen efficace de prévenir le

**Les faits**

Un plaignant croit que son fournisseur de télédiffusion par satellite se tient au courant des émissions qu'il regarde. Il est convaincu que le fournisseur demande aux clients de brancher leur ligne téléphonique en permanence dans l'appareil de réception dans le seul but de surveiller leurs habitudes de visionnement.

Dans la plainte déposée au Commissariat, il prétend que le fournisseur recueille et utilise à tort et à travers les renseignements personnels recueillis grâce à sa connexion téléphonique.

Le fournisseur a confirmé qu'il demande à ses clients de brancher leur ligne téléphonique en permanence dans l'appareil de réception qu'il leur fournit dans le but de facturer les services de télévision à la carte et d'éviter le piratage, pas pour surveiller les habitudes de visionnement. La compagnie a expliqué, et le Commissariat l'a confirmé, qu'il n'était pas possible avec la technologie actuelle de surveiller d'autres types d'émission que celles de la télévision à la carte, puisque la transmission par satellite est à sens unique et que les appareils de réception ne peuvent enregistrer d'autres émissions. L'entreprise ne dispose d'aucune autre information que celle concernant les services achetés par le client et les transactions électroniques effectuées au moyen du système de commande de télévision à la carte et elle recueille ces renseignements à des fins de facturation seulement.

En ce qui concerne la prévention contre le piratage, le Commissariat en a examiné les aspects techniques et a constaté que la connexion continue à une ligne téléphonique est un moyen de prévention efficace. Malgré les explications de l'entreprise, le plaignant continue de croire que celle-ci recueille plus de renseignements que nécessaire pour prévenir le piratage, mais il n'a pas été en mesure de fournir de preuves pour appuyer ses allégations.

**Nos conclusions**

Les fins de l'entreprise, soit la facturation des services de télévision à la carte et la prévention du piratage, sont des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Rien ne prouve que l'entreprise recueillait des renseignements sur les habitudes de visionnement de ses abonnés à partir de la connexion téléphonique. Les renseignements sur les émissions choisies et d'autres renseignements relatifs à la facturation ont été recueillis au moment de l'achat et non grâce à une ligne téléphonique.

personnels. L'entreprise a également mis sur pied un comité de protection de la vie privée qui a adopté une politique sur la protection des renseignements personnels concernant les clients et qui élabore une politique semblable pour l'ensemble de ses employés.

La plaignante s'est dite satisfaite du fait que son nom ait été retiré de la liste et que l'entreprise ait effectué les changements nécessaires à sa documentation.

### **Nos conclusions**

En vertu de l'article 30 de la *LRPDE*, disposition transitionnelle demeurée en vigueur les trois premières années, la Loi s'appliquait jusqu'en 2004 aux renseignements personnels qu'une organisation communique pour contrepartie à l'extérieur de la province. Même si l'entreprise en cause se trouve au Québec, le Commissariat a accepté d'examiner la plainte en vertu de la Loi, car la plaignante a prétendu que l'entreprise avait communiqué des renseignements qui la concernaient à l'extérieur de cette province en 2002, c'est-à-dire pendant que l'article 30 était encore en vigueur.

Au moment de la plainte, les documents promotionnels de l'entreprise contenaient un avis précisant que les noms et adresses de ses clients étaient partagés avec des sociétés tierces et faisaient état d'une procédure de retrait des listes à l'intention des clients. Cependant, l'avis et la procédure de retrait manquaient de clarté. L'information était dissimulée dans des rubriques dont les titres n'étaient pas représentatifs du contenu. Cet avis ne constituait pas un effort raisonnable de la part de l'entreprise pour s'assurer que la personne était clairement avisée des fins secondaires de la communication des renseignements personnels recueillis. Par conséquent, l'entreprise contrevenait au principe 4.3.2. de la Loi et le consentement de la plaignante n'était pas valable.

Néanmoins, comme la plaignante s'est montrée satisfaite du résultat de l'enquête, le Commissariat a conclu que la plainte était résolue.

### **Un fournisseur de télédiffusion par satellite présumé avoir surveillé les habitudes de visionnement de ses clients**

Quand le client se fait dire de garder son système satellite branché en tout temps, il s'attend au pire de la part de l'entreprise. Mais celle-ci a-t-elle vraiment l'intention de s'immiscer dans sa vie privée?



## L'avis d'échange de renseignements d'une société du Québec manque de clarté

Si une organisation a l'intention d'échanger les noms et les adresses de ses clients avec des tiers à des fins de marketing, elle doit en informer les clients, mais pas de n'importe quelle façon. Selon le principe 4.3.2 de la Loi, les organisations sont tenues de faire un « effort raisonnable » pour informer leurs clients de ces fins et présenter celles-ci d'une manière que les clients peuvent comprendre.

Dans le cas qui nous intéresse, l'entreprise a fourni cet effort, mais le Commissariat doit déterminer si cet effort était raisonnable. Le cas comporte également un aspect juridictionnel intéressant lié à une disposition transitoire de la LPRPD.

### Les faits

Quelques mois après avoir acheté des produits de beauté par téléphone d'un commerce au Québec, la plaignante a écrit à l'entreprise pour demander que son nom soit rayé de la liste de publipostage. Plusieurs semaines plus tard, en octobre 2002, son nom se trouvait toujours sur une liste transmise à un consultant de l'Ontario mandaté pour échanger et louer ses listes de clients à d'autres organisations.

Dans sa plainte au Commissariat, la personne allégué que l'entreprise a vendu son nom et son adresse à des tiers en Ontario, sans son consentement. Elle soulève aussi la question de la procédure permettant aux clients de retirer leur consentement au marketing des tierces parties.

L'entreprise explique que le nom de la plaignante figurait toujours sur la liste de publipostage en raison d'un délai administratif normal dans le traitement d'une demande de retrait. L'entreprise fait également remarquer que sa pratique d'échange de listes de noms et d'adresses de clients avec d'autres entreprises et sa procédure de retrait des listes sont décrites dans un document mis à la disposition de la clientèle dans les envois postaux et les catalogues.

Notre enquête a confirmé l'existence de ce document. Cependant, le titre dominant du document est « Garantie de remboursement » et les avis en question se trouvent sous les titres « Aidez-nous à préserver les ressources naturelles » et « Les soins de beauté c'est personnel ».

L'entreprise a supprimé le nom de la plaignante de ses listes de publipostage. À la suite de l'intervention du Commissariat, l'entreprise a modifié ses documents promotionnels pour les rendre plus compréhensibles. D'ores et déjà, un client peut simplement cocher une case sur le bon de commande pour éviter l'échange de ses renseignements

Pour cette raison, la plainte était non fondée.

De plus, puisque la banque a établi ses fins et limité la collecte des renseignements personnels à celles-ci, elle se conforme aux principes 4.2 et 4.4 de la Loi.

À titre de corporation étrangère contrôlée, la banque doit se conformer à la réglementation applicable de l'IRS. Elle doit notamment déclarer les revenus d'intérêt gagnés par les citoyens américains, mais n'est pas tenue de le faire pour les citoyens non américains. Pour assurer l'exactitude des renseignements fournis à l'IRS et pour protéger les renseignements personnels des citoyens américains, la banque a fait parvenir un formulaire de déclaration de compte à ses détenteurs de compte en leur demandant d'indiquer s'ils étaient citoyens américains ou non. Il s'agit d'une demande raisonnable à des fins qu'une personne raisonnable estimerait acceptables aux termes du paragraphe 5(3) de la Loi.

En ce qui concerne le fond de la plainte – c'est-à-dire, la collecte et l'utilisation de renseignements personnels – le Commissariat est d'avis que la banque ne place pas la loi étrangère au-dessus des intérêts des clients canadiens en matière de vie privée.

### **Nos conclusions**

Les plaignants allèguent que la banque les obligerait à consentir à la collecte et à l'utilisation de plus de renseignements personnels que nécessaire aux fins de fournir les services de compte.

La banque a expédié par la poste à tous ses détenteurs de compte de dépôts personnels une lettre explicative et un formulaire de déclaration de compte. La lettre mentionnait que si une détentricice ou un détenteur de compte omettait de déclarer qu'il n'était pas citoyen américain, son nom et son adresse ainsi que le montant du revenu d'intérêt accumulé seraient communiqués à l'IRS. La lettre décrivait également l'objet de la collecte de ces renseignements et la façon dont ils seraient utilisés.

Elle doit notamment communiquer les revenus d'intérêt accumulés dans les comptes (IRS) en ce qui concerne la communication de renseignements et les retenues fiscales. Elle doit notamment communiquer les revenus d'intérêt accumulés dans les comptes américains ou qui sont présumés l'être, compte tenu qu'ils n'ont pas précisé qu'ils n'étaient pas citoyen américain.

- En ce qui concerne le bien-fondé de l'utilisation de caméras dans les circonstances entourant les plaintes, la compagnie n'a présenté aucune preuve indiquant que les absences non autorisées du lieu de travail constituaient un problème persistant chez les plaignants ou chez d'autres employés. La compagnie n'a pas prouvé qu'elle avait eu recours à d'autres moyens portant moins atteinte à la vie privée pour gérer les absences non autorisées. Une personne raisonnable ne jugerait pas acceptable l'utilisation de caméras pour traiter un problème de productivité au travail. Dans les circonstances, l'utilisation contrevenait au paragraphe 5(3) de la Loi.

- Lorsqu'un employeur a des motifs de croire que le lien de confiance a été rompu, il peut entreprendre la collecte de renseignements aux fins d'enquête sans le consentement de l'intéressé. Cependant, le seul élément de preuve présenté par la compagnie indiquant un bris du lien de confiance est le témoignage de la personne qui a vu les employés en cause prendre place dans un véhicule privé. La compagnie reconnaît que les employés auraient pu quitter le lieu de travail avec l'autorisation de leur supérieur immédiat et que le gestionnaire qui a utilisé la caméra n'a déterminé *qu'après coup* que les employés avaient quitté le lieu de travail sans autorisation. Les caméras représentant une très grande ingérence dans la vie privée, la décision de les utiliser, même dans les circonstances énoncées à l'alinéa 7(1)b), doit être prise avec grande prudence et après mûre réflexion. S'il existe un moyen portant moins atteinte à la vie privée d'obtenir le même résultat, il faudrait choisir cette méthode en premier.

Le Commissariat a conclu que les plaintes étaient fondées.

### **Des clients d'une banque doivent déclarer leur citoyenneté**

La plainte, précisément au sujet d'une banque qui recueille et utilise des renseignements personnels, soulève une préoccupation générale à savoir si la banque place les exigences d'une loi étrangère avant les intérêts de ses clients canadiens en matière de vie privée.

### **Les faits**

Plusieurs détenteurs de compte se sont plaints d'avoir reçu une lettre type leur demandant d'indiquer s'ils étaient ou non citoyens américains.

En 2001, la banque est devenue une filiale indirecte d'une société de portefeuille basée aux États-Unis. Comme la banque est maintenant classée comme une « corporation étrangère contrôlée » aux fins de la loi américaine de l'impôt sur le revenu, elle doit

- Il n'y a aucun doute ici que l'utilisation courante des caméras dans le but de renforcer la sécurité sur les lieux de travail est appropriée, conformément au paragraphe 5(3) de la Loi. Les caméras ont été installées à la suite d'une analyse des risques, et leur utilisation avait l'appui du syndicat comme de la direction.
- La Loi ne limite pas la définition de l'expression « renseignement personnel » aux renseignements enregistrés. Elle définit clairement les renseignements personnels de manière à inclure tout renseignement concernant une personne identifiable. Les caméras recueillent effectivement des renseignements personnels sur les employés et ont servi à recueillir des renseignements personnels concernant les plaignants, à savoir le fait qu'ils aient quitté la cour de triage pendant les heures de travail.
- La Loi ne limite pas la définition de l'expression « renseignement personnel » aux renseignements enregistrés. Elle définit clairement les renseignements personnels de manière à inclure tout renseignement concernant une personne identifiable. Les caméras recueillent effectivement des renseignements personnels sur les employés et ont servi à recueillir des renseignements personnels concernant les plaignants, à savoir le fait qu'ils aient quitté la cour de triage pendant les heures de travail.

Le Commissariat conclut ce qui suit :

un précédent.

Loi. Il signale que les plaintes examinées soulèvent des questions susceptibles de créer les organisations respectent la Loi et en sensibilisant les organisations et le public à la instruire ces plaintes. Il a évoqué le rôle de premier plan qu'il joue en établissant si Le Commissariat a également refusé d'exercer le pouvoir discrétionnaire de ne pas Le Commissariat fait remarquer premièrement que la décision de la Cour fédérale invoquée par la compagnie de chemin de fer faisait l'objet d'un appel et que, par conséquent, il avait juridiction en la matière.

### **Nos conclusions**

Le Commissariat fait remarquer premièrement que la décision de la Cour fédérale invoquée par la compagnie de chemin de fer faisait l'objet d'un appel et que, par conséquent, il avait juridiction en la matière.

Le Commissariat conclut ce qui suit :

un précédent.

Loi. Il signale que les plaintes examinées soulèvent des questions susceptibles de créer les organisations respectent la Loi et en sensibilisant les organisations et le public à la instruire ces plaintes. Il a évoqué le rôle de premier plan qu'il joue en établissant si Le Commissariat a également refusé d'exercer le pouvoir discrétionnaire de ne pas Le Commissariat fait remarquer premièrement que la décision de la Cour fédérale invoquée par la compagnie de chemin de fer faisait l'objet d'un appel et que, par conséquent, il avait juridiction en la matière.

Le Commissariat conclut ce qui suit :

un précédent.

Loi. Il signale que les plaintes examinées soulèvent des questions susceptibles de créer les organisations respectent la Loi et en sensibilisant les organisations et le public à la instruire ces plaintes. Il a évoqué le rôle de premier plan qu'il joue en établissant si Le Commissariat a également refusé d'exercer le pouvoir discrétionnaire de ne pas Le Commissariat fait remarquer premièrement que la décision de la Cour fédérale invoquée par la compagnie de chemin de fer faisait l'objet d'un appel et que, par conséquent, il avait juridiction en la matière.



## Caméras sur les lieux de travail : l'importance de s'en tenir à des fins raisonnables

Dans le présent cas, le Commissariat appuie l'utilisation de caméras vidéo pour améliorer la sécurité sur les lieux de travail, mais il ajoute que l'utilisation non restreinte de ces caméras aux fins de surveillance de la productivité des employés ou de gestion des relations employeur-employés aurait un effet dévastateur sur le moral des employés. Les employés qui utilisent les caméras à des fins opérationnelles légitimes doivent s'efforcer de s'en tenir à ces fins, faire preuve de grande prudence et bien réfléchir avant de recourir à la surveillance vidéo pour les fins exceptionnelles autorisées par la Loi.

### Les faits

Une compagnie de chemin de fer utilise des caméras pour surveiller le mouvement des trains et informer les membres de son personnel de l'emplacement du train. La compagnie a installé les caméras après une analyse des risques et a convenu avec le syndicat des employés que les caméras sont nécessaires à des fins opérationnelles.

Un jour, le gestionnaire responsable des caméras a aperçu deux employés qui montaient dans une automobile. Il est allé à son bureau et s'est servi du zoom de la caméra pour voir si les employés quittaient le lieu de travail. La compagnie leur a ultérieurement imposé une mesure disciplinaire pour avoir quitté le travail sans permission. L'un des deux employés a déposé un grief contre la mesure disciplinaire dont il a fait l'objet, et le litige a été soumis à l'arbitrage. Les deux employés ont déposé une plainte au Commissariat, alléguant que la compagnie avait utilisé des caméras vidéo, qui servent habituellement à des fins opérationnelles, pour établir s'ils avaient quitté les lieux pendant les heures de travail.

La compagnie a d'abord soutenu que la commissaire devrait exercer son pouvoir discrétionnaire pour décider de ne pas émettre de rapport, puisque que la question était soumise à l'arbitrage. Invoquant ensuite une décision récente dans laquelle la Cour fédérale avait statué que les tribunaux du travail avaient compétence exclusive à l'égard des litiges découlant des conventions collectives, la compagnie a soutenu que le Commissariat à la protection de la vie privée n'avait pas juridiction dans ces cas.

La compagnie a également soutenu que la Loi permet aux organisations de recueillir, d'utiliser et de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. Elle a nié avoir réellement recueilli des renseignements personnels sur les plaignants lorsque le gestionnaire a ciblé la caméra sur eux puisque celle-ci n'enregistre pas. L'entreprise a décrit la

Plusieurs employés de la société ont porté plainte au Commissariat, alléguant que la société utilise les caméras pour recueillir des renseignements personnels les concernant, notamment sur leur comportement et leur rendement au travail.

L'employeur soutient qu'une note de service a été affichée pour informer les employés de l'installation des caméras et du but poursuivi, qui consiste à assurer la sécurité et le bien-être des employés en surveillant la circulation des personnes ne faisant pas partie du personnel à l'intérieur et à l'extérieur de l'édifice. Cependant, les employés ignoraient l'existence de cette note.

Pendant notre enquête, la société a convenu d'informer les employés des fins auxquelles les renseignements recueillis par les caméras de surveillance sont utilisés. Elle a aussi accepté d'élaborer un document de politique relative à l'utilisation des caméras, comprenant les buts, l'emplacement de l'équipement, le personnel autorisé à opérer le système, le temps de surveillance et d'enregistrement ainsi que les principes d'équité applicables.

La société a subséquemment rempli ses engagements.

### **Nos conclusions**

La société n'avait pas fait d'efforts raisonnables pour informer ses employés, contrevenant ainsi au principe 4.3.2 de la Loi.

L'enquête a par ailleurs démontré que l'utilisation d'un tel système de surveillance constituait un moyen approprié de protéger les employés. Puisque les caméras ne sont pas utilisées pour recueillir des renseignements personnels sur les employés et ne sont ni utilisées dans des endroits où il y a possibilité raisonnable d'atteinte à la vie privée, il ne semble pas approprié que l'employeur obtienne le consentement de ses employés pour les utiliser. Dans l'hypothèse où les caméras recueilleraient, par inadvertance, des renseignements personnels concernant les employés, l'employeur ne pourrait utiliser les renseignements ainsi recueillis sans le consentement des employés, que dans les circonstances prévues aux alinéas 7(2)a) et b) de la Loi (ces dispositions s'appliquent aux enquêtes judiciaires et aux urgences, respectivement).

La société s'étant engagée à informer les employés et à élaborer un document de politique, le Commissariat a conclu que les plaintes étaient résolues.

a embauché un enquêteur privé, l'entreprise lui a donné pour instructions de recueillir l'information désirée en ciblant autant que possible la collecte des renseignements personnels.

En somme, l'entreprise avait un motif raisonnable de croire que le plaignant enfreignait son contrat de travail et avait manifestement de la difficulté à obtenir l'information requise au su et avec le consentement de l'intéressé. Le Commissariat a accepté que l'entreprise s'appuie sur les alinéas 7(1)(b) et 7(2)(d) pour recueillir et utiliser des renseignements personnels sur le plaignant à son insu et sans son consentement. La plainte était non fondée.

Indépendamment des conclusions, le Commissariat a recommandé que l'entreprise officialise les mesures qu'elle a prises en élaborant une politique et des pratiques en matière d'utilisation de la vidéosurveillance. Une telle politique devrait tenir compte des éléments suivants :

- La vidéosurveillance ne devrait être utilisée qu'en dernier recours et n'être envisagée que lorsque tous les autres moyens de recueillir des renseignements personnels ont déjà été épuisés.
- La décision d'exercer une surveillance vidéo devrait être prise à un échelon très élevé de l'organisation.
- L'enquêteur privé devrait recueillir les renseignements personnels conformément à la Loi et être particulièrement attentif au principe 4.4 (limiter la collecte).

L'entreprise a donné suite à cette recommandation.

### **Caméras sur les lieux de travail : l'importance de préciser le but poursuivi**

Les employés ont naturellement tendance à protester contre la présence de caméras vidéo au travail. Toutefois, en étant disposé à parler du but poursuivi, l'employeur peut souvent atténuer les craintes des employés au sujet de la perte de la protection de la vie privée.

### ***Les faits***

Donnant suite à une recommandation d'un examen de sécurité des lieux, une société de radiodiffusion a installé trois caméras de surveillance sur ses lieux de travail, une à l'extérieur et deux à l'intérieur de l'édifice. La caméra extérieure couvre le stationnement et l'entrée de l'édifice et les caméras intérieures sont dirigées vers l'entrée intérieure et le couloir central.

Au Commissariat, le plaignant a prétendu que son employeur avait recueilli des renseignements personnels à son insu et sans son consentement au moyen de vidéosurveillance et qu'il les avait utilisés pour le congédier.

Pour justifier les mesures prises dans ce cas, l'entreprise s'est servie des alinéas 7(1)(b) et 7(2)(d) de la Loi. Ces dispositions permettent à une organisation de recueillir et d'utiliser des renseignements personnels à l'insu de l'intéressé et sans son consentement s'il est raisonnable de s'attendre à ce que la collecte effectuée au su et avec le consentement de l'intéressé puisse compromettre l'exactitude du renseignement ou l'accès à celui-ci, et si la collecte est raisonnable à des fins liées à une enquête sur la violation d'un accord ou la contravention d'une loi.

L'entreprise a maintenu que sa décision de recourir à la vidéosurveillance était le résultat d'une consultation avec une équipe restreinte de professionnels du milieu juridique, médical et des relations industrielles, ayant établi que cette mesure était nécessaire en dernier recours dans les circonstances. L'entreprise a fourni les renseignements sur les limites physiques du plaignant à l'enquêteur et lui a donné pour instructions de surveiller les activités du plaignant pendant une période assez longue pour avoir un tableau complet de ses capacités et établir une preuve solide, factuelle et irréfutable de son comportement frauduleux. L'entreprise a cependant admis ne pas avoir de règle ou de procédure officielle en place pour guider les gestionnaires dans de telles situations.

### **Nos conclusions**

Il ne fait aucun doute que l'entreprise a eu recours à la vidéosurveillance pour recueillir des renseignements personnels à l'insu et sans le consentement du plaignant. Il s'agit de déterminer si l'alinéa 7(1)(b) peut s'appliquer dans ce cas. Toutefois, cette exception ne peut être interprétée isolément. Parmi les facteurs à examiner, il faut se demander si l'organisation avait une preuve substantielle permettant d'établir le soupçon de bris de la relation de confiance, si elle pouvait démontrer qu'elle avait pris tous les autres moyens portant moins atteinte à la vie privée pour obtenir l'information nécessaire et si elle avait limité le plus possible la collecte de renseignements.

Dans les circonstances, le Commissariat est convaincu que le but de l'entreprise, c'est-à-dire déterminer si le plaignant enfreignait son contrat de travail en faisant une déclaration trompeuse sur son état de santé, était fondé sur une preuve substantielle. Par ailleurs, l'entreprise a eu recours à des moyens portant moins atteinte à la vie privée pour recueillir l'information dont elle avait besoin, mais le plaignant s'est opposé à la plupart de ces tentatives qui n'ont pas dissipé les doutes de l'organisation. Lorsqu'elle



personnels sur le plaignant sans son consentement, contrevenant au principe 4.3 de la Loi. La plainte était fondée.

### **La vidéosurveillance, en dernier recours**

Le Commissariat considère la vidéosurveillance comme une forme de technologie portant grandement atteinte à la vie privée. La nature même du médium permet la collecte de nombreux renseignements personnels, dont beaucoup sont liés à des tierces parties n'ayant commis aucun délit, sont parfois superflus ou mènent à des jugements sur la personne en cause qui n'ont rien à voir avec le but initial de la collecte d'information.

Les entreprises ne devraient recourir à la vidéosurveillance qu'en dernier recours à des fins d'enquête, notamment pour enquêter sur les employés à l'extérieur du lieu de travail.

### **Les faits**

Pendant qu'il était à l'emploi d'une entreprise, le plaignant a déclaré avoir subi des blessures liées au travail et a demandé que le lieu de travail soit adapté en raison de limites physiques. Pendant près de deux ans, l'entreprise a tenté de satisfaire ses demandes d'adaptation, mais sans résultat. Le plaignant était de moins en moins satisfait des efforts de la société, ne voulait pas accomplir ses tâches et s'objectait aux demandes répétées d'information médicale à jour.

Devant le comportement du plaignant et son manque de collaboration à fournir l'information exacte sur sa capacité d'accomplir les tâches liées à son emploi, l'entreprise a douté de plus en plus de l'étendue de ses limites physiques. Elle a exigé qu'il se soumette à une évaluation médicale indépendante, ce qu'il a d'abord refusé, puis il a finalement accepté. Les évaluateurs indépendants ont conclu que, même si le plaignant avait effectivement des limites physiques, il semblait y avoir de nombreux « obstacles non physiques » à son retour au travail. Les évaluateurs ont également signalé que d'autres tests fonctionnels ne permettraient probablement pas une évaluation juste des véritables capacités fonctionnelles du plaignant.

Deux mois plus tard, tandis que le plaignant était en congé, l'entreprise a embauché un enquêteur privé pour le surveiller dans le but de déterminer s'il avait dit la vérité au sujet de ses limites physiques. Après deux semaines, l'enquêteur a remis à l'entreprise un rapport et huit heures d'enregistrement vidéo montrant le plaignant en train d'accomplir des tâches qu'il prétendait ne pas pouvoir effectuer. Ayant la preuve que le plaignant n'avait pas dit la vérité au sujet de son état de santé, l'entreprise l'a congédié.

accessibles. Toutefois, l'université s'attend aussi à ce qu'une entreprise ou une organisation demande la permission de communiquer avec les membres d'une faculté à des fins qui ne sont pas liées à la promotion des intérêts de l'université.

L'article 2 de la Loi exclut précisément de la définition de renseignement personnel le nom, le titre d'un employé d'une organisation ainsi que les adresse et numéro de téléphone de son lieu de travail, mais ne mentionne pas l'adresse de courriel d'affaires d'un employé. Les alinéas 7(1)d) et 7(2)c.1) précisent qu'une organisation peut recueillir et utiliser des renseignements personnels à l'insu de l'intéressé et sans son consentement s'il s'agit de renseignements réglementaires auxquels le public a accès.

Aux fins de ces alinéas, le règlement précise que les renseignements auxquels le public a accès incluent le nom, le titre, l'adresse et le numéro de téléphone d'une personne qui figure dans un répertoire, une liste ou un avis à caractère professionnel ou d'affaires qui est accessible au public, si la collecte, l'utilisation ou la communication de ces renseignements est directement liée à la raison pour laquelle ils figurent dans le répertoire, la liste ou l'avis.

### **Nos conclusions**

Nous avons conclu premièrement, puisque l'article 2 ne mentionne pas l'adresse de courriel d'affaires parmi les types de renseignements exclus, qu'il s'agit d'un renseignement personnel aux fins de la Loi.

Il faudrait ensuite déterminer si l'organisation sportive pouvait invoquer les exceptions au consentement énoncées aux alinéas 7(1)d) et 7(2)c.1).

L'université a publié les adresses de courriel des facultés sur son site Web en espérant que les entreprises, les organisations et les personnes communiquent avec les membres des facultés dans le but de servir les intérêts de l'université. La vente de billets de saison pour une manifestation sportive n'est toutefois pas liée à ce but. Le même raisonnement s'applique au site Web du cabinet auquel le plaigant était associé. De plus, même après la première protestation du plaigant, l'organisation a obtenu son adresse courriel de cette autre source et l'a utilisée de nouveau à des fins de marketing, et ce, malgré la demande explicite du plaigant.

En somme, nous avons établi que l'organisation ne peut invoquer les exceptions au consentement puisqu'elle a recueilli et utilisé les renseignements personnels du plaigant à des fins sans rapport avec le motif pour lequel ces renseignements ont été publiés. Par conséquent, l'organisation a recueilli et utilisé des renseignements

Il est donc établi que l'entreprise a utilisé de manière inappropriée les renseignements personnels du plaignant en contrevenant au principe 4.3 de la Loi. La plainte était fondée.

### **Un professeur se plaint d'être inondé de courriels non sollicités à son bureau**

L'adresse courriel d'affaires d'une personne est-elle une pratique équitable pour les spécialistes du marketing?

#### **Les faits**

Le plaignant a reçu, à son bureau de l'université, un courriel non sollicité annonçant des billets de saison pour les parties d'une équipe professionnelle. L'agent vendeur en cause a admis avoir pris l'adresse électronique sur le site Web de l'université et il a accepté de ne plus envoyer de courriel au plaignant sans son consentement. Deux semaines plus tard, cependant, le plaignant a reçu un deuxième courriel de sollicitation provenant de la même organisation, mais d'un agent vendeur différent.

Le plaignant prétend que l'organisation a obtenu et utilisé ses renseignements personnels sans son consentement.

L'organisation n'a pas nié qu'elle avait envoyé au plaignant un courriel de sollicitation à l'adresse de son bureau à deux occasions. Les deux représentants des ventes en cause sont responsables d'un « programme » de sollicitation différent, le premier du « programme universitaire » et le second du « programme des spécialistes du droit ». L'agent responsable du programme des spécialistes du droit a conçu sa liste à partir du site Web d'un cabinet d'avocats auquel le plaignant était associé. Il n'y avait aucun système de concordance indiquant que le plaignant avait demandé de supprimer son nom des listes de marketing de l'organisation.

En réponse au plaignant, l'organisation a supprimé son nom de toutes ses listes de marketing et établi des contrôles de référence de vente pour assurer un traitement similaire pour toute objection éventuelle. L'organisation a aussi fait appel à une nouvelle entreprise de billetterie et de vente mieux renseignée sur les exigences de la

*LPRPDE.*

L'université en cause est d'avis que les adresses de courriel de son personnel constituent de l'information commerciale. L'université exige habituellement des membres des facultés qu'ils acceptent de publier leur adresse de courriel d'affaires, conformément à son modèle d'affaires et à son attente voulant que les employés soient facilement

en prononçant des paroles offensantes que l'entreprise a jugées passibles d'une mesure disciplinaire. Une enquête s'en est suivie et le plaignant a été congédié pour conduite inconvenante pour un employé (il a été réintégré depuis).

Le superviseur a déclaré au Commissariat qu'après avoir entendu les mots « test » et « clinique » utilisés par l'infirmière au cours de leur conversation téléphonique, il avait supposé que le plaignant participait à un programme de surveillance pour toxicomanes. De son côté, l'infirmière a affirmé avoir utilisé le mot « rendez-vous » et non pas « test ». Elle prétend n'avoir donné au superviseur que les renseignements nécessaires pour lui signifier qu'un taxi était nécessaire et qu'il y avait un motif raisonnable pour que l'entreprise paie la course.

À un certain moment, le directeur régional de l'entreprise a demandé à l'infirmière d'offrir sa version des faits quant à la mauvaise conduite présumée du plaignant. Elle l'a fait dans un courriel envoyé au directeur régional et achevé par la suite à deux autres cadres supérieurs. Dans le courriel, l'infirmière déclarait que le plaignant devait se soumettre à un « test médical ... pour vérifier s'il était toujours en état d'assumer sa tâche » et ce, dans les quatre heures suivant son appel téléphonique. Croyant que ce renseignement laissait supposer sa participation au programme, le plaignant a objecté que le renseignement avait été communiqué aux parties en question.

Le plaignant prétend que l'infirmière a communiqué de façon inappropriée ses renseignements personnels à son superviseur dans une conversation téléphonique et aux autres cadres supérieurs dans un courriel.

### *Nos conclusions*

Quant à la conversation téléphonique, bien qu'il semble pertinent que l'infirmière ait donné au superviseur un motif pour justifier l'appel d'un taxi, notre enquête n'a pas permis d'établir avec exactitude ce que l'infirmière avait dit au superviseur. Quels que soient les mots employés, ils ont laissé entendre au superviseur que le plaignant participait au programme de surveillance pour les toxicomanes ou, alors, ils ont simplement confirmé ses soupçons.

De même pour le courriel, nous ne contestons pas la nécessité d'informer les cadres supérieurs de la mauvaise conduite présumée du plaignant, mais le contenu de cette information pose problème. Puisque le but de l'infirmière était de relater le comportement du plaignant, il était superflu d'indiquer que ce dernier était tenu de se soumettre à un test médical dans les quatre heures. Les mots « rendez-vous chez le médecin » auraient été suffisants pour expliquer la nécessité de prendre un taxi.



## Cas choisis en vertu de la LPPDE

Fournir des réponses écrites aux demandes de renseignements exige beaucoup de temps et de main-d'œuvre. Au cours de l'année, l'Unité des demandes de renseignements a accumulé des arrières en raison de demandes de renseignements excédant le temps de réponse mensuel moyen. Avec la mise en place des nouvelles mesures, le Commissariat veillera à déterminer si les changements ont entraîné une hausse de l'efficacité.

Les cas suivants illustrent l'ampleur et l'éventail des cas faisant l'objet d'une enquête par le Commissariat. Nous avons diffusé 29 résumés de cas pour l'année 2004 sur notre site Web.

### Renseignements médicaux communiqués en raison d'un choix de mots indiscret

Même avec les meilleures intentions et lors d'activités apparemment sans conséquences, comme lorsqu'il s'agit simplement d'appeler un taxi, les professionnels de la santé doivent faire attention à ce qu'ils disent aux gestionnaires d'entreprise sur la santé des employés.

#### Les faits

Après avoir suivi un programme pour toxicomanes, le plaignant a signé un contrat de « dernière chance », condition pour conserver son emploi dans une entreprise de transport nationale. Ce contrat l'obligeait à se soumettre à une surveillance régulière, ainsi qu'à des tests de dépistage de consommation de drogue et d'alcool effectués au hasard par le fournisseur de services de santé de l'entreprise. Le plaignant était très préoccupé par la confidentialité et avait fait en sorte de cacher sa situation à ses collègues et à ses superviseurs.

Un jour, alors qu'il était en congé chez lui, il a reçu un appel d'une infirmière lui demandant de se rendre à la clinique dans les quatre heures afin de fournir un échantillon d'urine. Quand il a dit à l'infirmière qu'il ne pouvait pas y aller, celle-ci a répondu qu'elle appellerait l'entreprise et organiserait son transport en taxi. Peu de temps après, le plaignant recevait un appel de son superviseur lui disant qu'un taxi le conduirait au laboratoire. Le superviseur lui a ensuite demandé s'il était « sous contrat », laissant entendre qu'il faisait référence à un « contrat de dernière chance ».

En se fondant sur les paroles du superviseur, le plaignant a présumé que l'infirmière en avait trop dit à son sujet. Irrité par ce qu'il croyait être une communication de renseignements confidentiels le concernant, il a confronté l'infirmière et le superviseur

recherche de conseils en prévision de la mise en application intégrale de la *LPRPDE* le 1<sup>er</sup> janvier 2004.

Au cours de l'année, les pénuries de personnel dans l'Unité des demandes de renseignements, conjuguées au volume très élevé de travaux en cours, ont présenté des défis. À l'issue de quoi, il a été nécessaire de réévaluer la manière dont nous répondons aux demandes de renseignements du public. Le Commissariat n'accepte plus les demandes de renseignements ou les plaintes par courriel. Nous avons instauré un système téléphonique automatisé pour répondre aux questions du public les plus fréquemment posées, notamment celles concernant le vol d'identité, le telemarketing et, bien entendu, le numéro d'assurance sociale. En outre, nous continuons d'ajouter de l'information dans le site Web du Commissariat afin de répondre aux questions les plus fréquentes. Nous avons également affecté temporairement quelques enquêteurs pour qu'ils aident l'Unité. Enfin, nous invitons désormais les personnes à téléphoner pendant les heures de bureau ; nous pouvons souvent mieux déterminer, et de façon plus rapide, les besoins d'un demandeur en lui parlant au téléphone que par l'entremise d'une série de courriels et de lettres.

## STATISTIQUES CONCERNANT LES DEMANDES DE RENSEIGNEMENTS

Pour la période s'étendant du 1<sup>er</sup> janvier au 31 décembre 2004

Le tableau suivant représente le nombre total de demandes de renseignements concernant la *LPRPDE* auxquelles l'Unité des demandes de renseignements a répondu.

8 861	Demandes de renseignements par téléphone
3 271	Demandes de renseignements par écrit (lettre, courriel et télécopieur)
12 132	Nombre total de demandes de renseignements reçues

## Délais de réponse aux demandes de renseignements

En moyenne, les demandes de renseignements écrites (soit le quart de la charge de travail de l'Unité) ont reçu une réponse dans les trois mois. Par ailleurs, les demandes de renseignements effectuées par téléphone constituent presque les trois quarts des demandes de renseignements. La majorité de ces dernières ont reçu une réponse immédiate. Quant au reste des demandes ayant pu nécessiter des recherches, elles ont été traitées à l'intérieur d'une à deux semaines.

CONCLUSIONS PAR TYPE DE PLAINTE

Plaintes fermées entre le 1<sup>er</sup> janvier et le 31 décembre 2004

	Abandonnée	Réglée rapidement	Hors juridiction	Non fondée	Résolue	Réglée en cours d'enquête	Fondée	TOTAL
Accès	10	3	2	8	5	20	14	62 (16 %)
Responsabilité	0	0	0	0	0	1	0	1 (0 %)
Exactitude	2	1	0	1	0	1	0	5 (1 %)
Possibilité de porter plainte	0	0	0	0	0	0	1	1 (0 %)
Collecte	10	2	1	25	15	30	13	96 (25 %)
Consentement	2	1	0	0	0	3	1	7 (2 %)
Correction/Annotation	0	0	0	0	0	1	1	2 (1 %)
Frais	0	2	1	0	0	2	0	5 (1 %)
Conservation	0	0	0	0	1	1	0	2 (1 %)
Mesures de sécurité	0	0	1	2	0	13	2	18 (5 %)
Délais	0	0	0	2	1	3	1	7 (2 %)
Utilisation et communication	22	10	1	25	5	77	33	173 (46 %)
<b>TOTAL</b>	<b>46</b>	<b>19</b>	<b>6</b>	<b>63</b>	<b>27</b>	<b>152</b>	<b>66</b>	<b>379</b>
(# et %)	(12 %)	(5 %)	(2 %)	(17 %)	(7 %)	(40 %)	(17 %)	

Demandes de renseignements

L'Unité des demandes de renseignements répond aux demandes du public au sujet de la mise en application de la *LPRPDE* ainsi que de la *Loi sur la protection des renseignements personnels*. Le Commissariat reçoit des milliers de demandes de renseignements chaque année en provenance du public et d'organisations cherchant à obtenir des avis concernant la protection des renseignements personnels dans le secteur privé.

En 2004, le Commissariat a reçu 12 132 demandes de renseignements concernant la *LPRPDE*, soit moins qu'en 2003, alors qu'il en avait reçu 13 422. Cette diminution peut être attribuable à une meilleure compréhension de la *LPRPDE* par les organisations qui y sont assujetties. En 2003, par contre, bon nombre d'organisations étaient à la

## Définitions des conclusions en vertu de la LPRPDE

Le Commissariat a élaboré une série de définitions de ses « conclusions » pour expliquer les résultats de ses enquêtes menées en vertu de la LPRPDE :

**Non fondée** : L'enquête n'a pas permis de déceler des éléments de preuves qui suffisent à conclure qu'une organisation a enfreint les droits du plaignant en vertu de la LPRPDE.

**Fondée** : L'organisation n'a pas respecté une disposition de la LPRPDE.

**Résolue** : L'enquête a corroboré les allégations, mais l'organisation a pris les mesures nécessaires pour remédier à la situation, à la satisfaction du Commissariat, ou s'est engagée à prendre ces mesures correctives.

**Réglée en cours d'enquête** : Le Commissariat aide à négocier, en cours d'enquête, une solution qui convient à toutes les parties. Aucune conclusion n'est rendue.

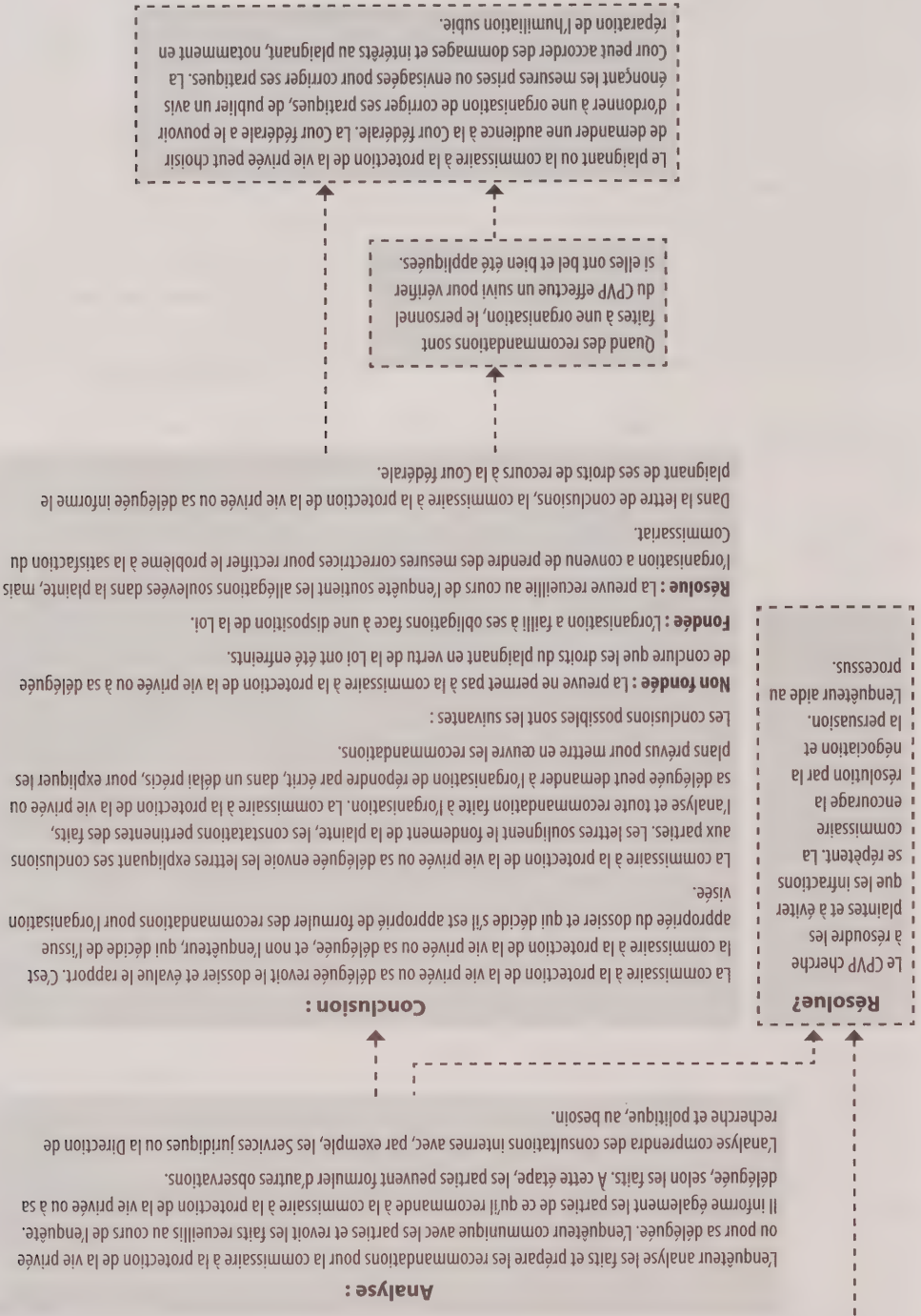
**Abandonnée** : Il s'agit d'une enquête qui est terminée avant que toutes les allégations ne soient pleinement examinées. Une affaire peut être abandonnée pour toutes sortes de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire ou il est impossible de lui demander de fournir des renseignements supplémentaires, qui sont essentiels pour en arriver à une conclusion.

**Hors juridiction** : L'enquête a montré que la LPRPDE ne s'applique pas à l'organisation ou à l'activité faisant l'objet de la plainte.

**Réglée rapidement** : Il s'agit d'un nouveau type de disposition. Elle s'applique aux situations lorsque l'affaire est réglée avant même qu'une enquête officielle ne soit entamée. À titre d'exemple, si une personne dépose une plainte concernant un sujet qui a déjà fait l'objet d'une enquête par le Commissariat et qui a été jugé conforme à la LPRPDE, nous expliquerons la situation à la personne plaignante. Cette conclusion est également utilisée lorsqu'une organisation, mise au courant des allégations, règle immédiatement la question à la satisfaction du plaignant et du Commissariat.



Note : une ligne brisée (---) indique un résultat possible.



## Processus d'enquête en vertu de la LRPPE

### Demande de renseignements :

Une personne communique avec le CVP par lettre, par téléphone ou en personne pour porter plainte contre une atteinte à la Loi. Les personnes qui prennent contact par téléphone ou en personne doivent par la suite présenter leurs allégations par écrit.

### Analyse initiale :

Le personnel des enquêtes examine l'affaire en cause afin de déterminer si elle constitue bel et bien une plainte, c.-à-d. d'évaluer si les allégations peuvent contrevenir à la Loi.

Une personne peut se plaindre de toute question énoncée aux articles 5 à 10 de la Loi ou à l'annexe 1 – par exemple, un refus de communiquer des renseignements personnels la concernant détenus par une organisation ou un retard inacceptable pour communiquer l'information ; la collecte, l'utilisation ou la communication inappropriée de renseignements personnels ; des erreurs dans les renseignements personnels utilisés ou dévoilés par une organisation.

### Plainte?

**Non :**  
La personne est informée, par exemple, que la question ne relève pas de notre organisme.

Un enquêteur est affecté au dossier.

**Oui :**

### Enquête :

L'enquête servira à établir si on a contrevenu au droit à la protection de la vie privée des personnes ou si on a permis aux personnes de recevoir la communication des renseignements personnels les concernant.

L'enquêteur écrit à l'organisation pour expliquer l'essentiel de la plainte. Il rassemble les faits se rapportant à la plainte par des observations des deux parties et par une enquête indépendante, des entrevues avec des témoins et une revue de la documentation. Au nom de la commissaire à la protection de la vie privée ou de sa déléguée, l'enquêteur a le pouvoir de recevoir des preuves, d'avoir accès à des lieux au besoin, et d'examiner ou d'obtenir des copies de dossiers trouvés sur place.

### Analyse (suite)

### Résolue? (suite)

### Abandonnée?

Une plainte peut être abandonnée si, par exemple, un plaignant décide de ne pas continuer avec sa plainte et si elle ne peut être localisée.

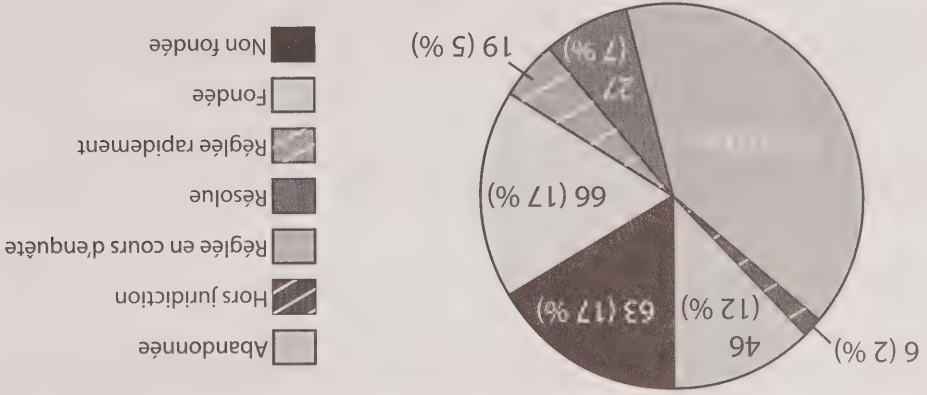
### Règlement rapide?

Une plainte peut être résolue avant qu'une enquête n'ait commencé si, par exemple, la question a déjà été traitée dans le cadre d'une autre plainte et si l'organisation a cessé la pratique.

## Définition des types de plaintes formulées en vertu de la LRPDP

Les plaintes que reçoit le Commissariat sont classées d'après les principes et les dispositions législatives de la LRPDP qui ont été présumentement enfreints :

- **Accès.** Une personne s'est vu refuser l'accès aux renseignements personnels qu'une organisation détient à son sujet ou n'a pas reçu tous les renseignements, soit en raison de l'absence de certains documents ou renseignements ou parce que l'organisation a invoqué des exceptions afin de soustraire les renseignements.
- **Responsabilité.** Une organisation a failli à l'exercice de ses responsabilités à l'égard des renseignements personnels qu'elle possède ou qu'elle garde ou elle a omis de désigner une personne responsable de surveiller l'application de la Loi.
- **Exactitude.** Une organisation a omis de s'assurer que les renseignements personnels qu'elle utilise sont précis, complets et à jour.
- **Possibilité de porter plainte.** Une organisation a omis de mettre en place les procédures ou les politiques qui permettent à une personne de porter plainte en vertu de la Loi ou elle a enfreint ses propres procédures et politiques.
- **Collecte.** Une organisation a recueilli des renseignements personnels non nécessaires ou les a recueillis par des moyens injustes ou illégaux.
- **Consentement.** Une organisation a recueilli, utilisé ou communiqué des renseignements personnels sans le consentement de la personne concernée ou elle a fourni des biens et des services à la condition que la personne consente à la collecte, à l'utilisation ou à la communication déraisonnable de renseignements personnels.
- **Correction/Annotation.** L'organisation n'a pas corrigé, à la demande d'une personne, les renseignements personnels qu'elle détient à son sujet ou, en cas de désaccord avec les corrections demandées, n'a pas annoté les renseignements afin d'indiquer la teneur du désaccord.
- **Frais.** Une organisation a exigé plus que des frais minimaux pour fournir à des personnes l'accès à leurs renseignements personnels.
- **Conservation.** Les renseignements personnels sont conservés plus longtemps qu'il n'est nécessaire aux fins du but qu'une organisation a déclaré au moment de la collecte des renseignements ou, s'ils ont été utilisés pour prendre une décision au sujet d'une personne, l'organisation n'a pas conservé les renseignements assez longtemps pour permettre à la personne d'y avoir accès.
- **Mesures de sécurité.** Une organisation n'a pas protégé les renseignements personnels qu'elle détient avec des mesures de sécurité appropriées.
- **Délais.** Une organisation a omis de fournir à une personne l'accès aux renseignements personnels qui la concernent dans les délais prévus par la Loi.
- **Utilisation et communication.** Les renseignements personnels sont utilisés ou communiqués à des fins autres que celles auxquelles ils avaient été recueillis, sans le consentement de la personne concernée, et l'utilisation ou la communication de renseignements personnels sans le consentement de la personne concernée ne font pas partie des exceptions prévues dans la Loi.



### PLAINTES TERMINÉES ENTRE LE 1<sup>ER</sup> JANVIER ET LE 31 DÉCEMBRE 2004 : TYPES DE CONCLUSIONS

Le fait que le Commissariat ait pu régler un si grand nombre de dossiers laisse entendre que les organisations et les plaignants accueillent favorablement la possibilité de résoudre les plaintes avec célérité et réalisme. La démarche convient bien au rôle d'ombudsman du Commissariat ; après tout, notre rôle consiste à aider les personnes à résoudre des problèmes. En même temps, nous devons naturellement veiller au respect des intentions politiques générales de la *LPRPD*. Le Commissariat, autant que le plaignant et l'organisation concernée, souhaite voir les dossiers réglés ; cependant, selon nous, l'enthousiasme pour le règlement des plaintes en cours d'enquête ne signifie pas le règlement des plaintes à tout prix. Nos enquêteurs travaillent en étroite collaboration avec les parties dans le cadre du processus de règlement afin de veiller à ce qu'on aborde les problèmes systémiques soulevés par une plainte.

Si nous examinons les données concernant les catégories de plaintes « réglées en cours d'enquête » et « réglées rapidement », nous pouvons voir que 45 p. 100 des plaintes que reçoit le Commissariat sont résolues sans avoir nécessité l'investissement en ressources impliquant une enquête complète. Il s'agit là d'une bonne nouvelle pour un organisme faisant face à une charge de travail croissante.

Le fait de désormais mettre l'accent sur le règlement des plaintes constitue un élément important face au grand nombre de plaintes que reçoit le Commissariat. Au cours de l'année, le règlement en cours d'enquête d'une plainte a pris, en moyenne, moins de temps que toute autre forme de résolution, sauf dans le cas des plaintes abandonnées (où, par exemple, le plaignant peut ne plus vouloir poursuivre sa demande ou ne peut être localisé) ou réglées rapidement, c'est-à-dire lorsque la question est traitée avant la tenue d'une enquête.



TEMPS DE TRAITEMENT DES PLAINTES EN VERTU DE LA LRPDE

Le tableau présente la durée moyenne du traitement d'une plainte à partir de la date de réception d'une plainte jusqu'à sa conclusion.

Par conclusion

Pour la période s'échelonnant du 1<sup>er</sup> janvier au 31 décembre 2004

Type de plaintes fermées	Temps de traitement moyen en mois
Réglée rapidement	2,9
Abandonnée	5,6
Réglée en cours d'enquête	7,2
Hors juridiction	7,8
Moyenne globale	8,3
Résolue	10,5
Non fondée	11,0
Fondée	11,0
Moyenne globale	8,3

Par type de plainte

Pour la période s'échelonnant du 1<sup>er</sup> janvier au 31 décembre 2004

Type de plainte	Temps de traitement moyen en mois
Frais	3,4
Exactitude	6,4
Consentement	6,9
Délais	8,1
Utilisation et communication	8,2
Accès	8,3
Mesures de sécurité	8,4
Correction/Annotation	8,5
Collecte	8,9
Conservation	9,5
Responsabilité	12,0*
Possibilité de porter plainte	12,0*
Moyenne globale	8,3

\* Le temps de traitement moyen pour ces deux types de plaintes représente en fait un cas pour chacune.

Le règlement des plaintes en cours d'enquête n'a rien de nouveau ; c'est plutôt le fait que le Commissariat mette désormais l'accent sur ce type de règlement qui s'avère nouveau. En 2003, les cas réglés en cours d'enquête représentaient 2 p. 100 de l'ensemble des dossiers. En revanche, sur 379 cas résolus en 2004, 152 (soit un peu plus de 40 p. 100) faisaient partie de la catégorie des plaintes « réglées en cours d'enquête ». Ce fut de loin la méthode la plus utilisée.

Les plaintes concernaient les sujets suivants :

#### Répartition par type de plainte

Type de plainte	Nombre	Pourcentage
Utilisation et communication	286	39,6 %
Collecte	172	23,8 %
Accès	112	15,5 %
Mesures de sécurité	40	5,5 %
Consentement	37	5,1 %
Exactitude	22	3 %
Correction/Annotation	11	1,5 %
Frais	12	1,7 %
Autres	4	0,6 %
Conservation	6	0,8 %
Responsabilité	9	1,2 %
Délais	9	1,2 %
Possibilité de porter plainte	1	0,2 %
Transparence	2	0,3 %
<b>Total</b>	<b>723</b>	<b>100 %</b>

Au cours de l'année 2004, le Commissariat a fermé 379 plaintes. Il s'agit d'une amélioration par rapport à l'année précédente, où il en avait fermé 278. Néanmoins, au cours de ces deux années, le Commissariat a reçu plus de plaintes qu'il n'en a fermé. Il y a donc un risque de créer des arriérés.

Le Commissariat prend présentement des initiatives pour régler la situation, entre autres en réaffectant des ressources et en revoyant la façon de mener ses enquêtes. Une des approches les plus prometteuses pourrait être le fait de mettre l'accent, depuis janvier 2004, sur une catégorie de règlement des plaintes intitulée « Régler en cours d'enquête ». Il s'agit de cas où, au cours de l'enquête, le Commissariat a aidé à trouver une solution satisfaisante pour l'ensemble des parties.

# Plaintes

En 2004, la *LPRPDE* était pleinement en vigueur et s'appliquait à l'ensemble des activités commerciales dans les provinces dépourvues de lois essentiellement similaires à la loi fédérale. Au cours de l'année, le Commissariat a connu une hausse soudaine des plaintes déposées en vertu de la *LPRPDE*; en effet, il a reçu 723 plaintes entre le 1<sup>er</sup> janvier et le 31 décembre, soit plus du double des 302 plaintes reçues l'année précédente. Comme l'indique le tableau de la page 34, l'augmentation du champ d'application de la Loi semble constituer un facteur important de l'accroissement des plaintes. Une fois de plus, ce sont les institutions financières qui ont le plus souvent fait l'objet de plaintes, comme on peut s'y attendre, en raison des grandes quantités de renseignements personnels qu'elles manipulent. Elles étaient suivies par le secteur des télécommunications, un autre secteur ayant souvent fait l'objet de plaintes au cours des dernières années. Par ailleurs, le Commissariat a reçu des plaintes concernant quatre nouveaux secteurs – l'assurance, les ventes, l'hébergement et les services professionnels – totalisant plus de 25 p. 100 des plaintes. Il reste à savoir s'il y aura d'autres augmentations du nombre de plaintes, à mesure que les Canadiennes et les Canadiens connaîtront mieux la Loi.

## PLAINTES REÇUES EN VERTU DE LA LPRPDE ENTRE LE 1<sup>er</sup> JANVIER ET LE 31 DÉCEMBRE 2004

### Répartition par secteur

Secteur	Nombre	Pourcentage
Institutions financières	212	29,3 %
Télécommunications	125	17,3 %
Assurances	82	11,3 %
Ventes	82	11,3 %
Transports	67	9,3 %
Santé	36	5 %
Hébergement	18	2,5 %
Professionnels	15	2,1 %
Services	10	1,4 %
Autres	76	10,5 %
Total	723	100 %

n'est pas toujours applicable pour plusieurs raisons commerciales fondées. Les lois régissant la protection des renseignements personnels dans le secteur privé en Colombie-Britannique et en Alberta traitent d'embellie cette question et établissent des règles visant à protéger les renseignements personnels des consommateurs dans le cas d'une fusion ou d'une acquisition. La *LPRPDE* devrait-elle faire de même?

## • Surveillance

• La *LPRPDE* confère à la commissaire les pouvoirs d'un ombudsman. En d'autres termes, la commissaire n'a pas le pouvoir de prendre un décret ni d'imposer une pénalité à l'encontre d'une organisation qui contrevient à la *LPRPDE*. Bien que nous soyons d'avis que le modèle de l'ombudsman fonctionne bien dans l'ensemble (en fait, même dans les juridictions qui ont le pouvoir de prendre un décret quant aux questions touchant à la protection des renseignements personnels, la grande majorité des cas sont réglés sans qu'il y ait recours au décret), nous sommes au fait que dans d'autres juridictions, les organismes de surveillance ont des pouvoirs d'application de la loi. Le Parlement souhaite peut-être se pencher sur les avantages et les désavantages des deux modèles dans son examen de la *LPRPDE* en 2006.

Il ne s'agit là que de quelques enjeux qui peuvent être examinés au cours de l'examen quinquennal de la Loi.



lacune, surtout si cette loi innove et qu'elle prévoit de nouveaux droits et de nouvelles obligations. Nous n'avons pas toutes les solutions pour remédier à ces lacunes, mais nous avons repéré plusieurs enjeux et, dans certains cas, suggéré des moyens possibles de les traiter.

## • Portée

- La portée de la *LPRPDÉ* est-elle efficace en regard des renseignements personnels concernant les employés? Bon nombre de plaintes qui nous sont adressées ont trait à la relation employeur-employé. Actuellement, la *LPRPDÉ* ne convient pas toujours à ce type de relation. Dans les lois de la Colombie-Britannique et de l'Alberta régissant le secteur privé, les renseignements concernant les employés sont assujettis à un ensemble de règles distinct.

- Il y a des chevauchements évidents entre la *LPRPDÉ* et le *Code canadien du travail* ainsi qu'entre le mandat du Commissariat à la protection de la vie privée et celui des arbitres du travail.

- Il subsiste une certaine incertitude quant à la distinction, s'il en est une, entre l'activité « commerciale », telle qu'elle est définie par la Loi, et les services « professionnels ».

- Ailleurs dans le présent rapport, nous décrivons un cas qui implique l'envoi non sollicité de courrier électronique de nature commerciale à une adresse électronique professionnelle. La définition énoncée par la loi sur les « renseignements personnels », qui exclut certains renseignements personnels d'ordre professionnel tels que l'adresse et le numéro de téléphone, devrait-elle être élargie pour inclure l'adresse de courrier électronique professionnelle?

## • Consentement

- Le consentement est au cœur de la *LPRPDÉ*. Il s'agit aussi d'une des questions les plus problématiques soulevées en vertu de la Loi. Par exemple, une organisation doit-elle obtenir le consentement de tous ses clients lorsqu'elle propose de communiquer les renseignements personnels qui les concernent dans le cas d'une fusion ou d'une acquisition? Il semble que ce soit ce que la Loi exige, mais cette exigence

La Loi de 2002 sur la sécurité publique, sans les changements recommandés par la commissaire, est entrée en vigueur le 11 mai 2004.

#### Amendements à d'autres lois

Les Règles de la Cour fédérale (1998) ont été adoptées avant la LPRPDE. C'est ce qui explique pourquoi la règle 304(1)c, qui traite du service d'avis de demande », ne faisait pas référence à la LPRPDE. Par conséquent, en février 2003, les services juridiques ont demandé que la règle 304(1)c soit amendée afin d'indiquer la nécessité d'aviser la commissaire à la protection de la vie privée chaque fois qu'une demande est présentée en vertu de la LPRPDE ainsi que de la Loi sur la protection des renseignements personnels.

Les Règles modifiant les Règles de la Cour fédérale (1998) sont entrées en vigueur le 29 novembre 2004 et ont été publiées dans la Partie II de la *Gazette du Canada*, le 15 décembre 2004 (DORS/2004-283). L'article 16 de ce document amende la règle 304(1)c) pour inclure la LPRPDE. Le libellé de cet article est maintenant le suivant :

[...] 304(1)c) si la demande est présentée en vertu de la Loi sur l'accès à l'information, la Loi sur la protection des renseignements personnels, la partie 1 de la Loi sur la protection des renseignements personnels et les documents électroniques ou la Loi sur les langues officielles, au commissaire compétent sous le régime de cette loi ; [...]

## Examen de la LPRPDE par le Parlement en 2006

Le Commissariat se prépare à l'examen de la LPRPDE par le Parlement, qui est prévu pour 2006. L'année 2006 peut sembler lointaine dans le contexte du présent rapport annuel de 2004, mais notre expérience des quatre dernières années en matière de surveillance de l'application de la loi nous a convaincus qu'il s'agissait du moment opportun pour se préparer, et que le Commissariat constitue également le lieu adéquat où commencer. Le Commissariat jouera un rôle actif dans l'élaboration de positions de principe visant à rendre le fonctionnement de la loi plus simple et plus efficace, tant pour les organisations que pour les personnes, et à veiller à ce que les pratiques équitables en matière d'information qui sont au cœur de la LPRPDE se traduisent dans la pratique.

Comme toute nouvelle loi d'importance, la LPRPDE comporte des lacunes. Il est difficile d'obtenir du premier coup une loi qui soit entièrement exempte de toute

# Évolution de la Loi sur la protection des renseignements personnels et les documents électroniques

## Modifications statutaires

### Amendements à la LPRPDE

La Loi de 2002 sur la sécurité publique<sup>1</sup> inclut deux amendements à la LPRPDE. Ces derniers ont pour effet de permettre aux organisations de recueillir et d'utiliser des renseignements personnels sans consentement afin de les communiquer lorsque la loi l'exige ou de les communiquer à des institutions gouvernementales si ces renseignements ont trait à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales.

La commissaire s'est présentée devant le Comité sénatorial permanent des transports et des communications, le 18 mars 2004, pour faire entendre ses préoccupations au sujet de ces amendements.<sup>2</sup> Dans sa déclaration au Comité, la commissaire soulignait que les amendements proposés à la LPRPDE autorisent les organisations à agir à titre d'agents de l'État en recueillant des renseignements personnels sans consentement dans le seul but de communiquer ces renseignements au gouvernement et à des organismes du maintien de l'ordre. Elle demandait que l'amendement proposé à la LPRPDE soit abandonné et exprimait ses inquiétudes quant au fait que le libellé de cette loi est si vaste qu'il s'applique à toute organisation assujettie à la LPRPDE et que l'amendement ne réduit pas la quantité de renseignements recueillis sans consentement ni n'impose de limites quant aux sources de renseignements.

<sup>1</sup> Voir [http://www.parl.gc.ca/PDF/37/3/paribus/chambus/house/bills/government/C-7\\_4.pdf](http://www.parl.gc.ca/PDF/37/3/paribus/chambus/house/bills/government/C-7_4.pdf)

<sup>2</sup> Voir [http://www.privcom.gc.ca/speech/2004/sp-d\\_040318\\_f.asp](http://www.privcom.gc.ca/speech/2004/sp-d_040318_f.asp)

erronés relèvent du commissaire à l'information et à la protection de la vie privée de l'Alberta, tandis que le Commissariat s'est occupé des questions systématiques de conservation des rapports de solvabilité.

Même si les pièges constitutionnels sont nombreux, nous espérons qu'en adoptant une approche pratique pour l'application des lois régissant la protection des renseignements personnels du Canada, nous serons en mesure d'offrir une protection adéquate de la vie privée au Canada.



ces provinces. Ce protocole énonce en partie la manière dont le Commissariat à la protection de la vie privée du Canada s'occuperait des plaintes avant et après que la loi d'une province est déclarée « essentiellement similaire à la loi fédérale ».

Ces protocoles d'entente sont affichés sur le site Web du Commissariat à la protection de la vie privée du Canada ([www.privcom.gc.ca](http://www.privcom.gc.ca)). Ce site Web ainsi que les sites des autres commissaires provinciaux à l'information et à la protection de la vie privée présentent de plus amples renseignements concernant les juridictions, y compris une fiche d'information.

Le Commissariat entretient depuis longtemps des rapports avec la Commission d'accès à l'information (CAI) au Québec. Le Québec a été la première province canadienne à adopter une loi sur la protection des renseignements personnels dans le secteur privé, en 1994. Afin de tirer parti de la riche jurisprudence qu'a connue le Québec depuis 1994, nous avons commandé un document examinant et résumant l'expérience du Québec à ce jour.

Afin que cette démarche s'avère aussi utile que possible pour l'ensemble des provinces et des territoires, nous avons constitué un comité de rédaction externe pour faciliter l'exécution de ce projet. Les membres de ce comité sont :

Madeleine Aubé, avocate générale, Commission d'accès à l'information du Québec

Jeffrey Kaufman, Fasken Martineau, Toronto

Mary O'Donoghue, avocate principale, Commissariat à l'information et à la protection de la vie privée de l'Ontario

Murray Rankin, Arvey Finlay, Victoria

Frank Work, c.r., commissaire à l'information et à la protection de la vie privée de l'Alberta

Ce document a été publié au mois d'août 2005 et est maintenant disponible sur notre site Web.

Le commissaire de l'Alberta et la commissaire fédérale ont déjà collaboré pour mener une enquête comportant des éléments fédéraux et provinciaux – voir par exemple, le sommaire de cas sur une enquête fédérale-provinciale concernant des renseignements médicaux envoyés par erreur, mentionné plus loin, sous la section des incidents visés par la *LPRPD*. Dans un autre cas, le service de police d'Edmonton a trouvé, dans le cours d'une enquête, des renseignements servant à déterminer les autorisations de sécurité des fonctionnaires de l'Alberta. Ces renseignements incluaient des rapports de solvabilité. Les parties de l'enquête ayant trait à la correction de rapports de solvabilité

Dans un autre cas, une personne travaillait pour une entreprise située dans une des provinces de l'Ouest qui dispose d'une loi essentiellement similaire à la loi fédérale. Par l'intermédiaire de l'entreprise, la personne avait accès à un Programme d'aide aux employés (PAE) en Ontario et s'est plainte de la communication de renseignements personnels par le PAF. Puisque l'Ontario n'avait pas encore de loi essentiellement similaire à la loi fédérale, la *LPRPDE* s'appliquait en Ontario. Mais s'agit-il d'une juridiction de l'Ontario – parce que le PAF se trouve en Ontario – ou d'une juridiction de la province de l'Ouest en vertu de la loi de cette province concernant le secteur privé?

### **Simplifier notre approche en matière de juridiction**

Les commissaires du Canada et des provinces unissent leurs efforts afin de trouver ensemble une solution aux problèmes de juridiction, et ce processus se déroule dans un esprit de collaboration, sans confrontations. Si quelques personnes saisissent les tribunaux d'affaires mettant en cause la juridiction, dans l'ensemble, ces enjeux peuvent largement être réglés grâce à la discussion. Nous cherchons dans chaque cas à établir le mécanisme le plus simple et le plus clair possible pour les personnes et les organisations.

La création d'un forum régional sur la protection des renseignements personnels par le secteur privé, en collaboration avec l'Alberta et la Colombie-Britannique, est un des moyens que nous avons trouvés pour simplifier notre approche en matière de juridictions et de questions connexes liées aux enquêtes. Ce forum fonctionne sous la direction des commissaires du Canada et des provinces/territoires et vise à coordonner et à harmoniser la supervision fédérale et provinciale du secteur privé au Canada. Des employés chevronnés du secteur des enquêtes et du secteur juridique provenant de chacun des commissariats participent à des téléconférences mensuelles et à des réunions semestrielles. Ce forum a plusieurs fonctions, dont la plus importante consiste à élaborer des procédures pour la détermination de la juridiction, le transfert des plaintes et la conduite d'enquêtes parallèles.

Les commissaires du Canada et des provinces/territoires ont concerté leurs efforts pour mettre au point des protocoles d'entente relativement au traitement des enquêtes en présence de juridictions qui se chevauchent. En mars 2004, la commissaire à la protection de la vie privée du Canada a envoyé un protocole d'entente aux commissaires à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique, et une lettre similaire au commissaire à l'information et à la protection de la vie privée de l'Ontario en janvier 2005, dans lequel elle confirmait les discussions entourant le règlement des plaintes relatives à des organisations de

offrent des soins de santé dans le privé. Bien que la *Personal Information Protection Act* (*PIPA*) de l'Alberta s'applique aux organisations du secteur privé, elle ne vise pas les renseignements personnels sur la santé, tels qu'ils sont définis dans la *HIA*, qui sont recueillis, utilisés ou communiqués à des fins liées aux soins de santé. Par conséquent, la collecte, l'utilisation ou la communication de renseignements personnels sur la santé effectuée par des professionnels œuvrant dans le secteur privé ne relève d'aucune des deux lois de l'Alberta. C'est donc la *LPRPDE* qui s'applique dans un tel cas.

En mars 2005, un projet de loi a été présenté devant l'assemblée législative de l'Alberta en vue de modifier la *PIPA* pour y inclure explicitement les activités des professionnels de la santé œuvrant dans le privé qui font la collecte, l'utilisation ou la communication de renseignements personnels sur la santé dans le cadre de services médicaux. La modification a depuis été adoptée et a permis de résoudre ce problème.

### **Circulation des renseignements personnels au-delà des limites provinciales**

Un autre aspect des questions de juridiction surgit lorsque les renseignements circulent au-delà des limites provinciales. Une organisation de l'Alberta peut communiquer des renseignements personnels à une autre organisation en Saskatchewan dans le cadre d'une activité commerciale. Une personne pourrait se plaindre de cet échange interprovincial au Commissariat. Par ailleurs, une personne qui désire se plaindre de la communication de renseignements personnels qui la concerne par une organisation de l'Alberta peut déposer sa plainte auprès du commissaire à l'information et à la protection de la vie privée de l'Alberta en vertu de la *PIPA* de l'Alberta. Toutefois, si cette personne désire se plaindre de la collecte de ses renseignements personnels en Saskatchewan, elle peut déposer sa plainte auprès de la commissaire à la protection de la vie privée du Canada puisque la Saskatchewan ne dispose pas d'une loi essentiellement similaire à la loi fédérale régissant les activités des organisations du secteur privé. Que la plainte soit déposée en Alberta, auprès du Commissariat ou auprès des deux, nous collaborerons ensemble pour coordonner nos efforts dans la mesure du possible.

La question de juridiction est parfois obscure. Dans le cadre d'une affaire dont est actuellement saisi le Commissariat, la plaignante travaillait pour une organisation située dans une des provinces de l'Ouest qui dispose d'une loi essentiellement similaire à la loi fédérale. L'organisation offrait une assurance-invalidité. La plaignante avait demandé à la société d'assurances, dont le siège social était situé au Québec, d'avoir accès à son dossier, qui était conservé à Toronto. La société d'assurance a indiqué que la *LPRPDE* s'appliquait. S'agissait-il ici de la loi appropriée ou ce cas relevait-il plutôt d'une loi provinciale?

et la Loi de l'Ontario s'appliquent aux renseignements personnels sur la santé dans le secteur privé. Comme ce fut le cas avec les lois s'appliquant au secteur privé en Alberta et en Colombie-Britannique, la *LPRPD* et la *LPRPS* de l'Ontario s'appliqueront aux renseignements personnels sur la santé dans le secteur privé jusqu'à ce que la *LPRPS* soit déclarée essentiellement similaire à la loi fédérale.

Il se peut que même une loi « essentiellement similaire à la loi fédérale » n'ait pas de portée suffisamment large pour éviter toute concurrence entre les différentes juridictions. Dans le cas de l'Ontario, par exemple, le décret ne visera pas toutes les entités visées par la *LPRPS* de l'Ontario. Le décret proposé pourrait s'appliquer aux règlements concernant les dépositaires de renseignements sur la santé. Par conséquent, la *LPRPS* serait la seule loi s'appliquant à la collecte, à l'utilisation et à la communication de renseignements personnels par ces dépositaires en Ontario.

Par contre, le décret ne s'appliquerait pas aux tierces parties qui reçoivent ces renseignements personnels des dépositaires de renseignements sur la santé. En ce qui a trait aux dépositaires de renseignements ne concernant pas la santé, la *LPRPS* possède uniquement des dispositions sur l'utilisation et la communication de renseignements personnels sur la santé. La *LPRPS* ne réglemente pas les autres obligations en matière de protection de la vie privée, comme la collecte, l'accès et les mesures de protection. Par conséquent, la *LPRPD* continuerait de s'appliquer pour ces activités.

Une manière simple d'éviter qu'il y ait des chevauchements entre les travaux des différents commissaires dans les secteurs des juridictions concurrentes consiste à conclure des ententes informelles définissant les tâches de chacun. Le Commissariat travaillera en étroite collaboration avec l'Ontario, comme il l'a fait avec la Colombie-Britannique et l'Alberta afin que les deux lois soient appliquées de manière aussi homogène que possible.

Même si une loi a été déclarée « essentiellement similaire » à la *LPRPD*, ce ne sont pas toutes les activités commerciales d'une province qui seront visées par ce décret, et les limites de la juridiction de chacune de ces lois ne seront pas toujours claires. Des questions complexes liées aux juridictions se poseront et il faudra une collaboration étroite entre les juridictions visées pour les résoudre.

Par exemple, la *Health Information Act (HIA)* de l'Alberta s'applique aux dispensateurs de soins de santé qui sont payés par le régime d'assurance-santé de l'Alberta pour offrir de tels soins. La *HIA* ne s'applique pas aux professionnels de la santé qui



deux lois – qui portent le même titre, soit *Personal Information Protection Act* – ont été adoptées par les assemblées législatives et sont entrées en vigueur le 1<sup>er</sup> janvier 2004.

En nous fondant sur les critères établis dans l'avis publié dans la *Gazette du Canada*, soit la présence des dix principes de l'annexe 1 de la *LPRPD*, un mécanisme de surveillance et de recours indépendant et une disposition limitant la collecte, l'utilisation et la communication des renseignements aux seules fins légitimes (le critère de la personne raisonnable), nous avons conclu que, dans l'ensemble, les lois de la Colombie-Britannique et de l'Alberta sont essentiellement similaires à la *LPRPD*.

Pour l'Alberta et la Colombie-Britannique, la gouverneure en conseil a émis deux décrets (C.R. 2004-1163, le 12 octobre 2004 et C.R. 2004-1164, le 12 octobre 2004) excluant les organisations visées par la loi provinciale. La *LPRPD* continue de s'appliquer aux entreprises fédérales ainsi qu'aux transactions interprovinciales et internationales.

## Juridictions

La *Loi sur la protection des renseignements personnels sur la santé* (LPRPS) de l'Ontario est entrée en vigueur le 1<sup>er</sup> novembre 2004. La *LPRPS* établit les règles relatives à la collecte, à l'utilisation et à la communication de renseignements personnels sur la santé pour les dépositaires de renseignements sur la santé en Ontario. Le Commissariat a informé Industrie Canada qu'il est d'avis que la *LPRPS*, qui touche les dépositaires d'information relative à la santé, est essentiellement similaire à la *LPRPD*. Industrie Canada a demandé au Commissariat son avis sur un projet de décret déclarant que la loi de l'Ontario est essentiellement similaire à la *LPRPD*, mais aucun décret final n'avait encore été pris au moment de mettre le présent rapport sous presse.

En Alberta et en Colombie-Britannique, les lois sur la protection des renseignements personnels s'appliquant au secteur privé étaient en vigueur durant la majeure partie de 2004, soit du 1<sup>er</sup> janvier au 12 octobre, mais celles-ci n'avaient pas encore été déclarées essentiellement similaires à la loi fédérale. Au cours de cette période, les deux lois sur la protection des renseignements personnels visant le secteur privé ainsi que la *LPRPD* s'appliquaient. Il y avait donc juridiction concurrente.

À partir du 1<sup>er</sup> janvier 2004, la *LPRPD* s'appliquait aux renseignements personnels dans le secteur privé en Ontario (sauf aux employés assujettis à la réglementation provinciale). La *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) est entrée en vigueur le 1<sup>er</sup> novembre 2004. Depuis cette date, la *LPRPD*

## Processus d'évaluation des lois provinciales et territoriales

Le 3 août 2002, Industrie Canada a publié un avis dans la *Partie I* de la *Gazette du Canada* qui établit la manière dont il déterminera si les lois provinciales ou territoriales sont réputées essentiellement similaires à la *LPRPDÉ*.

Une province, un territoire ou une organisation peut enclencher ce processus. À cette fin, il lui faut informer le ministre de l'Industrie de l'existence d'une loi qui, à son avis, est essentiellement similaire à la *LPRPDÉ*. Le ministre peut aussi agir de son propre chef et recommander à la gouverneure en conseil de désigner une loi provinciale ou territoriale comme étant essentiellement similaire à la loi fédérale. L'avis précise que le ministre sollicitera le point de vue de la commissaire à la protection de la vie privée et qu'il l'inclura dans sa présentation à la gouverneure en conseil. Le processus offre également une occasion au public et aux parties intéressées de formuler des observations sur les lois dont il est question.

Selon l'avis publié dans la *Gazette du Canada*, le ministre s'attend à ce que les lois essentiellement similaires à la loi fédérale des provinces ou des territoires comportent les éléments suivants :

- elles intègrent les dix principes de l'annexe 1 de la *LPRPDÉ* ;
- elles prévoient un mécanisme de surveillance et de recours indépendant et efficace comportant des pouvoirs d'enquête ; et
- elles restreignent la collecte, l'utilisation et la communication des renseignements personnels à des fins appropriées ou légitimes.

## Lois provinciales « essentiellement similaires à la loi fédérale » adoptées à ce jour

La *Loi sur la protection des renseignements personnels dans le secteur privé* de la province de Québec est entrée en vigueur, avec quelques exceptions, le 1<sup>er</sup> janvier 1994. Elle contient des dispositions détaillées qui augmentent le droit à la protection des renseignements énoncés aux articles 35 à 41 du *Code civil du Québec* et leur donnent force de loi. En novembre 2003, la gouverneure en conseil a pris un décret (C.P. 2003-1842, 19 novembre 2003) qui exclut certaines organisations de cette province, qui sont assujetties à la loi provinciale. La *LPRPDÉ* continue de s'appliquer aux entreprises fédérales ainsi qu'aux transactions interprovinciales et internationales.

En 2003, les provinces de la Colombie-Britannique et de l'Alberta ont voté des lois qui s'appliquent à toutes les organisations de ces deux provinces, sauf a) celles qui sont assujetties à d'autres lois provinciales en matière de protection des renseignements personnels et b) les entreprises fédérales visées par l'application de la *LPRPDÉ*. Les

# Lois provinciales essentiellement similaires à la loi fédérale

Conformément au paragraphe 25(1) de la *LPRPDE*, le Commissariat est tenu de rendre compte chaque année au Parlement de la mesure dans laquelle les provinces ont édicté des lois essentiellement similaires à la *LPRPDE*.

Depuis le 1<sup>er</sup> janvier 2004, la *LPRPDE* s'applique à toutes les activités commerciales. Toutefois, l'alinéa 26(2)*b*) permet à la gouverneure en conseil de prendre un décret qui soustrait certaines activités de l'application de la *LPRPDE*. Ce décret peut être pris si la province en question a adopté une loi jugée essentiellement similaire à la *LPRPDE*. Ce décret peut exclure une organisation, une catégorie d'organisations, une activité ou une catégorie d'activités de l'application de la *LPRPDE* à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels assujettis à cette loi qui s'effectue à l'intérieur de la province en cause.

Le but de cette disposition est de permettre aux provinces et aux territoires de réglementer les pratiques de gestion de renseignements personnels des organisations faisant affaire à l'intérieur de leurs frontières, tout en assurant la protection homogène et efficace des renseignements personnels partout au Canada.

Si la gouverneure en conseil prend un décret déclarant la loi d'une province essentiellement similaire à la loi fédérale, la collecte, l'utilisation ou la communication de renseignements personnels par des organisations assujetties à la loi provinciale ne seront pas régies par la *LPRPDE*. Les transactions interprovinciales et internationales seront visées par la *LPRPDE* et celle-ci continuera également de s'appliquer, dans les limites d'une province, aux entreprises fédérales, ce qui comprend les banques, les compagnies aériennes, les radiodiffuseurs et les entreprises de télécommunications.

Les projets ayant bénéficié d'un financement total de 371 590 \$ comprennent :

PROJETS FINANÇÉS

50 000 \$	Rehausser le niveau de protection de la vie privée Évaluer et élaborer les pratiques exemplaires en matière de protection de la vie privée pour aider les entreprises à mieux traiter les renseignements personnels des clients en vertu de la LRPPE	Association canadienne du marketing Toronto, Ontario	École nationale d'administration publique (ENAP) Québec, Québec	Université Queen's Kingston, Ontario	La Freedom of Information and Privacy Association de la C.-B. Vancouver, Colombie-Britannique	Universités de l'Alberta et de Victoria Edmonton, Alberta Victoria, Colombie-Britannique Université de Toronto Toronto, Ontario	Services basés sur l'emplacement : analyse des répercussions sur la vie privée dans le contexte canadien Répercussions sur la protection de la vie privée pour les services fondés sur l'emplacement géographique — questions soulevées et grands défis et conseils pour favoriser l'observation Le défi de l'identification des consommateurs aux nouvelles méthodes de paiement par voie électronique Méthodes actuelles et nouvelles méthodes proposées d'identification des consommateurs au paiement par voie électronique et aux facteurs de risque	17 100 \$	Les droits à la protection de la vie privée et les services de communications payés d'avance : évaluer la question de l'anonymat Justification et faisabilité des mesures de règlementation en vue d'élimer la vente de services de communications anonymes payés d'avance au Canada	14 850 \$	Université Simon Fraser Vancouver, Colombie-Britannique	Université Dalhousie Halifax, Nouvelle-Écosse	Analyse des répercussions juridiques et technologiques sur la protection de la vie privée des technologies d'identification par radiofréquence Étude de la technologie d'identification par radiofréquence et impact sur la vie privée et mesures juridiques pour protéger la vie privée	14 603 \$
-----------	---	---	--	---	--	---	--	-----------	---	-----------	--	--	---	-----------

Ces projets seront complétés en 2005. Des liens vers les résultats de ces projets seront affichés sur notre site Web.



# Recherche sur les nouveaux enjeux liés à la protection de la vie privée

Le 1<sup>er</sup> juin 2004, le Commissariat a officiellement lancé un programme des contributions afin d'appuyer la recherche des groupes sans but lucratif (comme les établissements scolaires, les associations industrielles et commerciales, les organisations de consommateurs, les organismes bénévoles et de défense des droits) sur la protection des renseignements personnels et sur les façons de protéger ces derniers. Ce programme est un jalon dans le développement d'une capacité nationale de recherche dans ce domaine au Canada. Il a été conçu pour aider le Commissariat à sensibiliser davantage la population et à mieux lui faire comprendre les enjeux de la protection de la vie privée.

Le programme des contributions de 2003-2004 en place mettait l'accent sur deux grandes priorités. La première consistait à étudier de quelle façon et dans quelle mesure les nouvelles technologies portent atteinte à la vie privée. Ces technologies comprenaient la surveillance vidéo, les dispositifs d'identification par radiofréquence, la technologie de repérage et la biométrie. Bon nombre de ces technologies sont plus menaçantes pour la vie privée lorsqu'elles sont utilisées par les gouvernements, mais elles représentent aussi une grave menace lorsqu'elles sont utilisées par le secteur privé.

La deuxième priorité du programme de recherche était plus directement liée à la mise en œuvre de la *LPRPD*, surtout depuis que de nouveaux secteurs de l'économie sont assujettis à cette loi, soit depuis janvier 2004. Cette partie du programme des contributions mettait l'accent sur la connaissance et la promotion de bonnes pratiques relatives à la protection de la vie privée comme élément clé d'un comportement commercial responsable.

à un gouvernement étranger ou à un organisme à la suite d'une ordonnance directe rendue par un tribunal étranger. En fait, dans bien des cas, l'organisation canadienne contrefaitrait la *LPRPD* si elle communiquait ces renseignements sans le consentement des personnes auxquelles ils se rapportent.

Toutefois, si une organisation communiquait des renseignements en vertu d'une loi canadienne telle que la *Loi sur l'aéronautique*, qui autorise les transporteurs aériens canadiens à communiquer à d'autres pays des renseignements sur les passagers, elle n'aurait pas à l'encontre de la *LPRPD*.

Nous jugeons aussi qu'une organisation qui exerce ses activités dans un pays étranger et qui détient des renseignements sur des Canadiennes et des Canadiens *dans ce pays* doit se soumettre aux lois de celui-ci. Ce qui signifie que lorsqu'une organisation canadienne impartit le traitement des renseignements personnels aux États-Unis ou à tout autre pays, il est possible qu'on ait accès à ces renseignements en vertu des lois de ces pays.

Evidemment, le gouvernement étranger pourrait demander ces renseignements par le biais d'un traité d'entraide juridique et demander au ministre fédéral de la Justice de faire en sorte que les organismes chargés d'appliquer la loi au Canada obtiennent pour eux ces renseignements auprès de sociétés canadiennes. Ce système de collaboration entre gouvernements est antérieur à la *USA PATRIOT Act*.

La *LPRPD* traite de façon succincte de la question de la circulation transfrontalière des données au principe 4.1.3 de l'Annexe de la Loi. Selon ce principe, l'information transmise à des fins de traitement doit être protégée dans une mesure « comparable » à celle de la *LPRPD*. Cependant, lorsque des données sont détenues ou traitées à l'extérieur du Canada, il est impossible de contrôler ce que ces pays font de cette information et le Commissariat n'a aucune autorité de surveillance.

Il faut s'occuper de toute urgence du problème de la circulation des renseignements personnels afin d'assurer la protection des renseignements personnels que nous transmettons partout dans le monde. Au début de l'année 2005, la diffusion d'une série d'articles de presse et de reportages au sujet d'entreprises étrangères détenant des renseignements personnels sur des Canadiennes et des Canadiens, coupables d'atteinte à la sécurité, a fait ressortir l'importance d'exercer une vigilance sur la circulation transfrontalière des données au Canada.

et concernant beaucoup de gens, il y a de fortes chances que leurs décisions soient fondées sur de faux renseignements ou sur des renseignements qui sont examinés hors contexte.

L'utilisation malveillante, la fausse interprétation ou la communication inappropriée de renseignements personnels peut avoir de graves conséquences sur les personnes, les familles et même les collectivités concernées. Le problème s'aggrave lorsque, en raison des dispositions relatives au secret et du manque de transparence, nous ne sommes pas en mesure de déterminer où se trouve la faille dans le système ou pourquoi ces personnes ont été injustement visées.

## L'impartition et la circulation transfrontalière des renseignements personnels

La question de la transmission vers l'étranger de renseignements personnels à partir du Canada (circulation transfrontalière des données) remonte à la même époque que les lois sur la protection des renseignements personnels. Les spécialistes et les experts en politique gouvernementale des années 60 et 70 préoyaient que le progrès de la technologie des communications entraînerait une plus grande circulation de données. Mais auraient-ils pu prévoir que la circulation de données à l'échelle planétaire prendrait l'ampleur qu'elle a aujourd'hui?

En 2004, en Colombie-Britannique, une plainte a été déposée au sujet de l'impartition des renseignements personnels sur la santé du gouvernement vers une entreprise américaine œuvrant sur son territoire. C'est à ce moment que la question de la circulation transfrontalière des renseignements personnels est devenue d'actualité au Canada. Le syndicat des employés du gouvernement de la Colombie-Britannique a déclaré que le gouvernement américain aurait accès à ces renseignements grâce à l'extension des pouvoirs de fouille établie par la *USA PATRIOT Act* en 2001. Même si beaucoup de cas d'impartition des renseignements personnels ont retenu l'attention du public depuis les dernières années, soulevant parfois des inquiétudes quant à leurs conséquences sur la protection des renseignements personnels, il semble que ce soit le premier cas où une loi particulière constitue un danger. Par la suite, le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, David Loukidelis, a fait la démarche d'inviter le public à soumettre ses commentaires sur cette affaire, et nous avons répondu à l'appel en présentant un mémoire.

Notre soumission expliquait qu'une entreprise détenant des renseignements personnels sur des résidents canadiens au *Canada* n'est pas tenue de fournir ces renseignements

Le problème du couplage des données n'est pas nouveau et préoccupe les spécialistes de la protection des renseignements personnels et les organismes de surveillance depuis plus de vingt ans. La technologie ayant évolué, nous ne parlons plus réellement de couplage des données, mais plutôt du forage des données. De nombreuses utilisations invisibles sont faites des systèmes intégrés d'information qui recueillent et analysent un grand nombre de renseignements personnels liés à nos tendances touristiques, à nos opérations financières et même aux gens que nous fréquentons. Si les consommateurs connaissaient et comprenaient bien ces systèmes, ils les verraient d'un bon œil puisque, grâce à eux, les demandes de prêt sont approuvées plus rapidement, les vols de cartes de crédit sont détectés instantanément et le service à la clientèle s'est amélioré. Toutefois, ces systèmes analysent désormais aussi une tonne de renseignements personnels dans le but de découvrir des activités qui laisseraient supposer qu'une personne menace la sécurité, blanchit de l'argent ou contribue au financement d'un groupe de terroristes. Puisque les organismes chargés de l'application de la loi et les agences de sécurité nationale recueillent beaucoup de renseignements provenant de nombreuses sources

sécurité est une autre question d'intérêt pour le Commissariat.

En juillet 2004, le gouvernement du Canada a commencé à appliquer de nouvelles normes de sécurité maritime en vertu du Code international pour la sûreté des navires et des installations portuaires (Code ISPS) de l'Organisation maritime internationale. Afin d'accroître la sécurité maritime, Transports Canada propose l'instauration d'un Programme d'accès aux zones réglementées des infrastructures maritimes, programme controversé qui vise à vérifier les antécédents des employés des ports pouvant entrer dans les zones à accès restreint. Dans le cadre de cette procédure, une quantité importante de renseignements personnels et susceptibles d'être confidentiels sera recueillie auprès de 30 000 employés des ports. La mesure dans laquelle les bases de données de renseignements du secteur privé doivent servir à ces vérifications de sécurité est une autre question d'intérêt pour le Commissariat.

plaintes.

d'obtenir des réponses pour être en mesure de donner suite à leurs requêtes et à leurs plus en plus préoccupant pour les Canadiennes et les Canadiens et nous essayons des renseignements personnels sont courantes au Canada, mais il s'agit d'un sujet de Nous ne savons pas dans quelle mesure ces pratiques d'utilisation et de conservation maintien de l'ordre et la lutte contre le terrorisme fait toujours l'objet de critiques. données du secteur privé et la conservation des renseignements personnels pour le qu'il pourrait jouer en matière de sécurité. Aux États-Unis, l'utilisation de bases de aussi nous interroger sur notre capacité à bien surveiller le secteur privé et le rôle sécurité de l'infrastructure essentielle. Du point de vue du Commissariat, nous devons



En 2004, le Commissariat a exprimé ses inquiétudes à propos d'une disposition de la Loi de 2002 sur la sécurité publique qui modifie la LPRPDE. Cette modification autorise les organisations assujetties à la LPRPDE à recueillir des renseignements personnels sans consentement afin de les communiquer au gouvernement, aux organismes chargés d'appliquer la loi et aux agences de sécurité nationales si ces renseignements ont un lien avec la sécurité nationale, la défense du Canada ou la conduite des affaires internationales. Le fait de permettre aux organisations du secteur privé de recueillir des renseignements personnels sans consentement les enrôle effectivement dans des activités de maintien de l'ordre et brouille dangereusement la ligne de démarcation entre le secteur privé et l'État. Dans le Rapport annuel concernant la Loi sur la protection des renseignements personnels, les questions liées à la sécurité publique sont abordées plus en profondeur, mais cette question est aussi importante du point de vue de la LPRPDE, car il y a un risque que les données du secteur privé soient manipulées incorrectement pour servir les intérêts de l'État.

La Loi antiterroriste de 2001 comprenait une disposition concernant la tenue d'un examen après trois ans. Le Sénat a nommé un comité spécial pour procéder à cet examen. À la Chambre des communes, cet examen est effectué par le Sous-comité de la sécurité publique et nationale, un sous-comité du Comité permanent de la justice et des droits de la personne, de la sécurité publique et de la protection civile. Cependant, ce comité ne tient pas compte des nombreuses autres lois qui ont aussi été édictées ou amendées dans la foulée des attentats terroristes. Bon nombre de ces lois possèdent un grand pouvoir d'intrusion et devraient aussi être révisées.

En 2001, la Loi sur les secrets officiels a été remplacée par la Loi sur la protection de l'information. L'article 10 de la nouvelle loi autorise l'administrateur d'un ministère, après obtention d'un certificat, à astreindre les membres du secteur privé au secret à perpétuité concernant les méthodes d'enquête ou les opérations spéciales. Nous comprenons que cette procédure peut s'avérer nécessaire lorsque la sécurité nationale et l'infrastructure essentielle sont menacées, mais afin d'assurer la responsabilité, nous sommes l'alarme lorsque se présentent de nouveaux pouvoirs sans dispositions de surveillance complémentaires. Nous avons soulevé la question de la responsabilité et de la surveillance dans notre présentation au Parlement portant sur l'examen de la Loi antiterroriste, mais la disposition visée figure dans la Loi sur la protection de l'information, et nous estimons que la fréquence de son utilisation doit être rendue publique.

Dans la lutte contre le terrorisme, les gouvernements ont clairement souligné la nécessité d'une coopération du secteur privé pour assurer la sécurité publique et la

## Sécurité nationale

Afin d'agir efficacement à titre d'agent du Parlement, nous sommes d'avis qu'il faut entretenir de bonnes relations de travail avec les ministères et les organismes fédéraux. Le CPVP prévoit mettre davantage l'accent sur l'identification et la communication des préoccupations en matière de protection de la vie privée au moment où le gouvernement élabore certaines initiatives, plutôt que d'attendre qu'elles fassent leur entrée au Parlement, afin d'accroître les chances que ces préoccupations soient prises en considération.

En mai 2004, on a édicté la *Loi de 2002 sur la sécurité publique*. Cette loi, présentée pour la première fois en novembre 2001 dans la foulée des attentats terroristes du 11 septembre, autorise le ministre des Transports, le commissaire de la GRC et le directeur du Service canadien du renseignement de sécurité (SCRS) à demander aux transporteurs aériens et aux exploitants de systèmes de réservation de services aériens de leur fournir, sans mandat, des renseignements sur les passagers. Cette mesure peut paraître justifiée compte tenu des risques que représentent les terroristes pour le transport aérien, mais l'utilisation qu'en font les autorités n'est pas seulement liée à la lutte antiterroriste ou à la sécurité des transports. La *Loi de 2002 sur la sécurité publique* permet aussi d'utiliser ces renseignements pour identifier les passagers recherchés en vertu d'un mandat et pour un large éventail d'infractions criminelles ordinaires. En d'autres mots, le mécanisme de la lutte antiterroriste sert à combler les lacunes de l'application ordinaire de la loi, nivelant par le bas le modèle généralement exigé des autorités responsables de son application.

Le gouvernement, qui conserve et exploite les données recueillies par le secteur privé, lance un message troublant aux organisations de ce secteur qui tentent d'observer les lois relatives à la protection des renseignements personnels. Si le gouvernement a le droit d'utiliser des données pour gérer les risques que peuvent représenter les personnes, pourquoi le secteur privé ne pourrait-il pas en faire autant? Afin de se conformer à la *LPRPD*, les entreprises privées recueillent de moins en moins de données. Mais le gouvernement leur demande maintenant de conserver les renseignements recueillis de sorte qu'il puisse y avoir accès à des fins gouvernementales. La *LPRPD* fixe la barre haute pour les organisations lorsqu'il s'agit d'utiliser et de communiquer des renseignements personnels sans consentement pour enquêter sur une fraude ou sur d'autres activités illégales qui ont des répercussions. Par contre, les normes auxquelles le gouvernement doit se conformer en vertu de la *Loi sur la protection des renseignements personnels* sont beaucoup moins rigoureuses.

plans de la promotion et de la protection du droit à la vie privée. L'objectif : ériger des ponts entre le CPVP et les ministères afin de leur faire part de nos observations plus tôt dans le processus législatif, au moment où nos commentaires peuvent être pris en compte de manière plus efficace. Lorsqu'un projet de loi a été déposé à la Chambre des communes, il est souvent trop tard pour repenser la façon d'aborder les enjeux en matière d'information.

Cette année, le Commissariat a répondu à une vaste correspondance et de nombreuses demandes de renseignements de sénateurs et de députés. La commissaire et les commissaires adjoints ont également rencontré en privé les sénateurs et les députés qui souhaitaient discuter de questions de politiques en matière de protection de la vie privée ou mieux connaître le fonctionnement du Commissariat.

### ► *Priorités pour l'année qui vient*

Le Commissariat prévoit une charge de travail élevée dans le domaine des affaires parlementaires pour le prochain exercice. De nombreux projets de loi d'intérêt pour le CPVP sont attendus au cours de la prochaine session, et l'examen parlementaire prévu par la loi de la *Loi sur la protection des renseignements personnels et les documents électroniques* doit débiter en 2006. Le CPVP prévoit jouer un rôle constructif au cours de cet examen en conseillant judicieusement les parlementaires qui feront l'étude du fonctionnement de la Loi au cours de ses premières années de mise en application, et des modifications et améliorations possibles.

Le CPVP continuera de suivre avec intérêt l'examen parlementaire de la *Loi antiterroriste*. Au cours de l'exercice 2005-2006, la commissaire à la protection de la vie privée s'est présentée à deux reprises devant des comités à ce sujet, d'abord devant un Comité spécial du Sénat procédant à l'examen de la Loi (9 mai 2005), ensuite devant un sous-comité du Comité permanent de la justice de la Chambre des communes (1<sup>er</sup> juin 2005).

En 2004, le CPVP s'est présenté devant des comités parlementaires traitant des projets de lois suivants :

- Projet de loi C-6, *Loi sur la procuration assistée* (3 mars 2004)
- Projet de loi C-7, *Loi de 2002 sur la sécurité publique* (18 mars 2004)
- Projet de loi C-2, *Loi modifiant la Loi sur la radiocommunication* (6 mai 2004)
- Projet de loi C-12, la *Loi sur la quarantaine* (18 novembre 2004)
- Projet de loi C-22, *Loi constituant le ministère du Développement social et modifiant et abrogeant certaines lois* (9 décembre 2004)
- Projet de loi C-23, *Loi constituant le ministère des Ressources humaines et du Développement des compétences et modifiant et abrogeant certaines lois* (9 décembre 2004)
- Projet de loi C-11, la *Loi sur la protection des fonctionnaires dénonciateurs d'actes répréhensibles* (14 décembre 2004)

En ce qui concerne la gestion et les opérations du Commissariat, les représentants du CPVP se sont présentés devant les comités parlementaires en 2004 pour discuter des sujets suivants :

- Rapport annuel et budget principal des dépenses 2003-2004 (17 novembre 2004)
- Budget supplémentaire des dépenses (1<sup>er</sup> décembre 2004)

#### ► *Autres activités de liaison avec le Parlement*

Le CPVP a lancé plusieurs autres initiatives au cours de la dernière année dans le but d'offrir de meilleurs conseils au Parlement sur des enjeux en matière de protection de la vie privée.

En mai 2004, nous avons créé une fonction de liaison avec le Parlement afin d'améliorer nos relations avec le Parlement. Cette fonction relève de la Direction de la recherche et politique et reflète la volonté du CPVP de cibler ses activités parlementaires de façon à fournir aux députés et aux sénateurs des conseils éclairés et judicieux sur les politiques.

L'une des priorités de la dernière année a été d'améliorer notre façon d'évaluer, de surveiller et de prévoir l'activité parlementaire. Le CPVP a instauré un nouveau système amélioré pour suivre de près l'évolution des projets de loi au Parlement et pour rester à l'affût de nouveaux développements qui présenteraient un intérêt sur les



## Guichet du Parlement pour la protection de la vie privée

Livres, il est difficile de contrôler les possibilités d'abus et d'atteinte à la vie privée. Les Canadiens et les Canadiennes doivent s'informer d'avantage et participer aux débats sur les enjeux pour la protection de la vie privée liés à ces nouveautés. Il faut que notre avenir soit le reflet des droits et des libertés que nous chérissons aujourd'hui. De Reginald Fessenden à Marshall McLuhan, les Canadiennes et les Canadiens ont été des chefs de file en ce qui a trait à l'élaboration de technologies et de théories dans le domaine des communications. Nous sommes confiants que nous pouvons relever le défi et démontrer que nous pouvons utiliser ces puissants dispositifs dans un monde où les ordinateurs et les communications sont omniprésents tout en respectant la plus fondamentale des valeurs humaines que représente la protection de la vie privée.

À titre d'agente du Parlement, la commissaire à la protection de la vie privée relève directement du Sénat et de la Chambre des communes. Ainsi, le CPVP tient lieu de guichet du Parlement sur les questions de protection de la vie privée. Par l'entremise de la commissaire, des commissaires adjoints et des autres représentants du CPVP, le Commissariat porte à l'attention des parlementaires les enjeux ayant une incidence sur le droit à la protection de la vie privée des Canadiennes et des Canadiens. Pour ce faire, le CPVP dépose des rapports annuels au Parlement, se présente devant les comités du Sénat et de la Chambre des communes afin d'expliquer les répercussions des mesures législatives et des initiatives gouvernementales proposées sur la protection de la vie privée, et de dégager et d'analyser les enjeux qui, à son avis, doivent être portés à l'attention du Parlement.

Le Commissariat aide également le Parlement à être mieux informé en ce qui concerne la protection de la vie privée en agissant à titre de ressource ou de centre d'expertise sur ces questions. À ce titre, il doit répondre à une vaste correspondance et à de nombreuses demandes de renseignements de sénateurs et de députés.

### ► *Présentations devant les comités parlementaires*

Les présentations devant les comités du Sénat et de la Chambre des communes constituent un élément clé de notre rôle de guichet du Parlement sur des questions de protection de la vie privée. Au cours de la période visée par ce rapport, la commissaire à la protection de la vie privée et les autres représentants du CPVP se sont présentés neuf fois devant des comités parlementaires : six fois pour des projets de loi ayant une incidence sur la protection de la vie privée et trois fois pour des questions ayant trait à la gestion et aux activités du Commissariat.

lecteurs biométriques. Ces dispositifs peuvent être « actifs » ou « passifs ». On les dit actifs lorsqu'ils peuvent transmettre de l'information à un lecteur de façon autonome, et passifs lorsqu'ils sont inactifs jusqu'à ce qu'un « lecteur » leur envoie un signal d'activation.

Ensemble, les étiquettes (qui peuvent être plus petites qu'un grain de riz ou dissimulées dans l'emballage d'un produit), les systèmes de codage puissants et les systèmes informatiques de pointe ont fortement incité les entreprises à utiliser les dispositifs d'identification par radiofréquence. Selon une étude de marché récente, la valeur du marché total des étiquettes d'identification passera de 1,95 milliard de dollars en 2005, à 26,9 milliards en 2015. Considérant qu'on pourra un jour se procurer une étiquette d'identification pour quelques sous seulement, l'ampleur de l'utilisation de ces étiquettes pourraient être plus grande que celle de presque toutes les autres technologies.

Les organisations doivent songer sérieusement aux implications juridiques de l'utilisation des dispositifs d'identification par radiofréquence. Toutefois, dans le tourbillon d'activités liées à ces dispositifs, peu nombreux sont ceux qui sont pleinement conscients des conséquences juridiques de la mise en place d'un tel système. À l'heure actuelle, les dispositifs d'identification sont utilisés par beaucoup d'entreprises et selon nous, nous devrons bientôt enquêter sur des plaintes liées à leur utilisation à des fins de repérage.

Dans le même ordre d'idées, même si les médias diffusent des histoires intéressantes à propos de l'utilisation abusive des systèmes mondiaux de localisation, la plupart des gens ne savent pas quelles données ces systèmes peuvent contenir. Heureusement, la *LPRPDI* comprend une disposition novatrice qui exige la transparence dans les pratiques liées aux renseignements personnels.

Les organisations qui fixent des dispositifs mondiaux de localisation aux biens de consommation ou aux moyens de transport (les voitures de location, par exemple) doivent établir la fonction du dispositif, les données que ce dernier recueille, combien de temps elles sont conservées et qui y a accès.

Nous sommes à l'aube d'un monde où la puissance informatique sera présente dans presque tous les dispositifs d'usage courant. Si nous ne sommes pas vigilants, cette puissance sera utilisée pour rassembler ou pour diffuser des renseignements personnels, ce qui portera gravement atteinte à la protection de la vie privée, ainsi qu'à notre autonomie et à notre dignité humaine. Comme on trouve les dispositifs de transmission le long des routes, sur les plaques d'immatriculation, la monnaie et les

**E**n 2004, nos principales préoccupations politiques portaient sur l'augmentation des demandes de renseignements personnels au nom de la sécurité nationale, à la circulation transfrontalière des renseignements personnels et, encore une fois, aux technologies portant atteinte à la vie privée. Des téléphones cellulaires dans les vestiaires aux systèmes mondiaux de localisation (GPS) dans les voitures, le besoin de mesurer l'incidence de ces nouvelles technologies et d'y intégrer les dispositions des lois relatives à la protection des renseignements personnels au moment de leur conception et de leur application est un défi continu.

## Technologie

Au cours de la dernière année, l'utilisation de dispositifs d'identification par radiofréquence (RFID) à des fins de repérage a eu des conséquences de plus en plus graves sur la protection de la vie privée. Les technologies RFID englobent des dispositifs qui utilisent habituellement les ondes radio pour lire un numéro de série enregistré sur une micropuce. Cette micropuce ou étiquette peut être fixée sur du matériel militaire, des passeports, des vêtements, des billets de monnaie, des véhicules, des pneus, des laissez-passer et sur presque tout ce qui se vend sur le marché, y compris les emballages de nourriture et de boisson. Entre autres fonctions, l'étiquette d'identification par radiofréquence permet de repérer des biens depuis le fabricant jusqu'au magasin de détail, de repérer une personne dans un établissement sanitaire ou de surveiller les déplacements d'un écolier.

Selon les caractéristiques de chaque modèle, les dispositifs d'identification par radiofréquence peuvent acheminer de l'information sur de longues distances ou sur quelques centimètres seulement. Ils peuvent garder en mémoire une multitude de renseignements personnels ou ne pas en garder du tout, et ils peuvent aussi servir de





# Notre mandat aux multiples facettes

Le Commissariat à la protection de la vie privée veille au respect de deux lois : la *Loi sur la protection des renseignements personnels*, qui s'applique aux institutions du gouvernement fédéral, et la *LPRPDE*, qui régit la gestion des renseignements personnels dans le cadre des activités commerciales.

Le Parlement a investi le Commissariat du mandat de veiller à ce que le secteur public fédéral et le secteur privé (dans la plupart des provinces) rendent compte du traitement qu'ils font des renseignements personnels, et à ce que le public soit informé de son droit à la protection de la vie privée. Ce mandat n'est pas toujours compris.

En sa qualité d'ombudsman indépendant, le Commissariat agit à titre :

- *d'enquêteur* et de *vérificateur* possédant les pleins pouvoirs d'enquêtes et pouvant déposer des plaintes, mener des activités de vérification et s'assurer du respect des deux lois ;
- de *sensibilisateur du grand public* et de *défenseur*, ayant la double responsabilité de sensibiliser les entreprises à leurs obligations en vertu de la *LPRPDE*, et d'aider le public à comprendre son droit à la protection de ses données personnelles ;
- de *chercheur* et d'*expert* des enjeux en matière de protection de la vie privée auprès du Parlement, du gouvernement et des entreprises ;
- de *défenseur des principes en matière de protection de la vie privée* dans les litiges ayant trait à l'application et à l'interprétation des deux lois régissant la protection des renseignements personnels. Nous analysons également les répercussions des projets de loi et des propositions gouvernementales sur les lois et les politiques.



Cette année, nous publions deux rapports afin d'établir une distinction entre la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels (LPRPDE). Cela nous semblait plus juste, compte tenu que la Loi sur la protection des renseignements personnels nous oblige à suivre l'exercice financier (2004-2005), alors qu'en vertu de la LPRPDE, nous sommes tenus de faire rapport en observant l'année civile (2004). De plus, chaque loi fournit un cadre distinct en ce qui a trait aux enquêtes et aux vérifications. Les deux rapports décrivent les efforts que nous avons déployés pour répondre aux attentes toujours plus nombreuses à l'égard du Commissariat pour que nous agissions, au nom du Parlement, à titre de gardiens de la protection de la vie privée des Canadiennes et des Canadiens. Les deux rapports se recoupent en plusieurs endroits, car un grand nombre de nos activités ne se rapportent pas spécifiquement à une loi ou à l'autre et, de plus en plus, les questions de politiques de politiques partagent des dénominateurs communs aux deux régimes.

## Répondre à un besoin grandissant

Du 1<sup>er</sup> janvier au 31 décembre 2004, le Commissariat a reçu 723 plaintes en vertu de la *LPRPDE*, soit plus du double des 302 plaintes reçues l'année précédente. Il a également réglé beaucoup plus de cas, soit 379 plaintes contre 278 en 2003. Même si on se questionne toujours sur le bien-fondé du rôle de la commissaire qui agit à titre d'ombudsman – rôle qui ne lui accorde pas le pouvoir de prendre des décrets – il est clair que le Commissariat a bien des réalisations positives à son actif grâce à l'approche actuelle de l'ombudsman. Au cours de l'année 2004, 40 p. 100 des plaintes dont l'enquête est terminée ont été réglées et 7 p. 100 ont été résolues, ce qui montre bien que la prise de conscience, une caractéristique dominante de l'approche de l'ombudsman, est un outil efficace.

Nous avons instauré une procédure générale de suivi systématique des enquêtes relatives aux plaintes formulées en vertu de la *LPRPDE*. Nous serons dorénavant en mesure de surveiller le progrès des organisations dans la mise en œuvre des engagements que celles-ci prennent durant ces enquêtes et dans le suivi des recommandations que leur transmet le Commissariat. La Direction de la vérification et de la revue du Commissariat est à renforcer sa capacité de vérification auprès des organisations assujetties à la *LPRPDE*, ce qui est tout aussi important.

Nous avons relevé plusieurs défis en 2004 et ces défis ne deviendront que plus nombreux et plus complexes. Pour ceux qui sont préoccupés par ce droit fondamental de la personne qu'est le droit à la vie privée, ce n'est pas le moment d'avoir peur de parler, ni d'avoir peur des débats ou de la controverse. Nous profiterons de l'examen de la *LPRPDE* en 2006 pour formuler des recommandations sur la façon d'améliorer et de mieux appliquer les deux lois sous notre gouverne. Même si l'application de la *LPRPDE* n'en est qu'à ses débuts, nous devons, compte tenu de l'évolution continue du milieu de la politique sur la protection des renseignements personnels, nous maintenir à jour et veiller à ce que les lois répondent efficacement aux menaces actuelles. Nous rédigeons présentement une liste d'améliorations et de propositions de changements, et nous sommes confiants que dans cinq ans, lors du prochain examen, d'autres modifications seront nécessaires. Le Parlement a eu la sagesse d'appuyer l'inclusion d'un examen périodique de la *LPRPDE*. En ce qui a trait à la *Loi sur la protection des renseignements personnels*, nous allons continuer à promouvoir son examen et l'inclusion du processus d'examen dans la loi elle-même.



de ses alliés dans la lutte contre le terrorisme, de consulter ces renseignements à des fins de « sécurité » signifie que l'on pourra avoir accès aux données imparties pour des raisons liées à l'application de la loi ou à la sécurité nationale hors de notre juridiction et de la protection consentie par nos lois et notre système judiciaire.

La circulation transfrontalière des données fait l'objet de discussions au Canada depuis les années 60. Le rapport intitulé *Ordonnateur et vie privée*, publié en 1972 par les ministères des Communications et de la Justice, abordait cette question en profondeur, y compris les enjeux liés à la souveraineté. La question a incité l'Organisation de coopération et de développement économiques (OCDE) à élaborer les premières Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel en 1980, puis l'Union européenne a adopté la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Pourtant, nous savons très peu de chose sur la circulation transfrontalière des renseignements personnels de la population canadienne et des clients d'entreprises canadiennes.

L'intérêt actuel pour la *USA PATRIOT Act* a soulevé une question litigieuse que l'on raisait depuis des dizaines d'années : dans quelle mesure les entreprises et les gouvernements canadiens devraient-ils communiquer des renseignements personnels à des gouvernements étrangers? Ce débat est loin d'être terminé. En fait, il ne fait que commencer. Le Commissariat a appuyé nombre des recommandations du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, David Loukidellis, sur les questions concernant la circulation transfrontalière des renseignements personnels et nous poursuivrons notre travail afin de nous assurer que les Canadiennes et les Canadiens conservent leurs protections en matière de renseignements personnels.

Le Commissariat a la responsabilité de protéger la vie privée au Canada. Cependant, il ne peut pas accomplir cette tâche seul. Nous comptons sur tous les intervenants de la société pour nous aider à préserver les droits et les libertés qui sont inhérents à la richesse de l'histoire du Canada et de son tissu social. La complexité de l'environnement actuel en matière de protection des renseignements personnels a incité le Commissariat à lancer un programme des contributions qui vise à appuyer l'élaboration d'une capacité nationale de recherche sur la protection de la vie privée au Canada. Les résultats de cette première série de projets de recherche seront communiqués en 2005. Ces résultats compléteront les recherches en politiques menées par le Commissariat et, de façon modeste, enrichiront le milieu de l'enseignement de la protection des renseignements personnels au Canada.

Il ne faut pas oublier que l'information c'est le pouvoir et que le détenteur de renseignements personnels détient un pouvoir considérable. Une des complexités à laquelle nous avons fait face cette année provient de la convergence de deux phénomènes, qui ne sont pas du tout nouveaux mais qui ont atteint un point critique. D'une part, l'impartition des activités de traitement des données et des centres d'appels signifie que les renseignements personnels des Canadiennes et des Canadiens et des clients d'entreprises canadiennes sont transférés et traités à l'étranger. D'autre part, la soit grandissante des gouvernements étrangers, en particulier celui des États-Unis et

de recherche de plus en plus complexes. Cela représente tout un défi.

Il ne peut parfois être impopulaire et qui exige une vaste expertise dans des domaines nous qui tentent de protéger ce droit fondamentalement clamer la tenue d'un débat répondre aux préoccupations mondiales actuelles en matière de sécurité. Ceux d'entre d'obtenir des renseignements personnels pour améliorer l'efficacité administrative et à propos des consommateurs et des employés, et la nécessité pour le gouvernement entreprises qui incite celles-ci à obtenir et à utiliser plus de renseignements personnels de surveillance et de manipulation des données, la concurrence mondiale entre les composer avec plusieurs éléments puissants : le progrès fulgurant des technologies L'environnement dans lequel nous revenons notre droit à la vie privée doit Univers complexe et changeant

des politiques.

privée du Canada en chevauchant leurs efforts pour mener des enquêtes et élaborer gaspiller le peu de ressources dont disposent les commissaires à la protection de la vie la protection des renseignements personnels et nous ne voulons certainement pas la tâche de ceux qui doivent se conformer aux nombreuses lois canadiennes régissant les juridictions provinciales et fédérales sont en cause. Nous ne voulons pas compliquer travaillons de pair avec nos collègues provinciaux pour simplifier les enquêtes lorsque provinciaux et de l'industrie, ces problèmes commencent à s'estomper. Nous Toutefois, grâce à la mobilisation des efforts du Commissariat, de nos homologues peuvent relever de la LPPDE.

tandis que d'autres, comme la communication interprovinciale des renseignements, c'est le cas pour la collecte de renseignements personnels à l'intérieur d'une province, des renseignements personnels peuvent être assujettis à une loi provinciale, comme cause dans l'examen d'une question. Quelques-uns des facteurs relatifs au traitement fédéral. Dans d'autres cas, il se peut aussi que les lois de deux juridictions soient en au traitement des renseignements personnels, à savoir la loi provinciale ou la loi peut s'avérer difficile de déterminer quelle loi s'applique à certaines pratiques relatives

## Avant-propos



En 2004, la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* a atteint sa pleine vigueur à la suite de l'élargissement de son application à toutes les activités commerciales du pays, à l'exception des provinces ayant des lois réputées être essentiellement similaires à la loi fédérale. La Colombie-Britannique, l'Alberta et le Québec ont promulgué des lois relatives à la protection des renseignements personnels dans le secteur privé, qui sont considérées comme « essentiellement similaires » à la *LPRPDE*. Cette loi s'applique aux entreprises fédérales du Canada ainsi qu'aux transactions interprovinciales et internationales.

Il y a de quoi se réjouir de la pleine vigueur de la *LPRPDE*. Les Canadiennes et les Canadiens bénéficient maintenant de droits étendus en matière de protection des renseignements personnels dans le secteur privé, et ils sont protégés depuis longtemps dans le secteur public grâce à la *Loi sur la protection des renseignements personnels* et aux lois provinciales correspondantes. Cela ne signifie pas que les lois visant le secteur privé et le secteur public en matière de protection des renseignements personnels préservent entièrement et de tous points de vue le droit des Canadiennes et des Canadiens à la vie privée. Ce n'est pas le cas. Cependant, la majeure partie du cadre essentiel à la protection de ce droit est maintenant en place. Le Commissariat continuera de veiller à et d'analyser l'application de la *LPRPDE* afin de s'assurer que cette dernière dessert bien les Canadiennes et les Canadiens et que le secteur privé canadien comprend et respecte ses obligations qui en découlent. Nous continuerons à aider le secteur des affaires à s'y conformer et nous élaborerons des pratiques exemplaires qui permettront de réduire le fardeau et de préciser les attentes.

## Défis intergouvernementaux

Comme pour toute loi relativement nouvelle, des difficultés peuvent survenir. Lorsqu'une province édicte une loi essentiellement similaire, en tout ou en partie, à la *LPRPDE*, il

<b>Plaintes .....</b>	<b>33</b>
Processus d'enquête en vertu de la LRPDP.....	38
Définitions des conclusions en vertu de la LRPDP.....	40
Demandes de renseignements.....	41
Cas choisis en vertu de la LRPDP.....	43
Choix de cas réglés en vertu de la LRPDP.....	59
Incidents en vertu de la LRPDP.....	68
Suivi des enquêtes sur les plaintes en vertu de la LRPDP.....	73
<b>Vérification et examen .....</b>	<b>79</b>
Renforcer la fonction de vérification .....	79
À l'affût de l'identification par radiofréquence.....	81
<b>Devant les tribunaux .....</b>	<b>83</b>
Requêtes en vertu de la LRPDP.....	83
Contrôle judiciaire.....	93
<b>Sensibilisation du grand public et communications .....</b>	<b>95</b>
<b>Gestion intégrée.....</b>	<b>99</b>
Vers le renouveau institutionnel.....	99
Renseignements financiers.....	103



# Table des matières

Avant-propos.....	1
Notre mandat aux multiples facettes .....	7
Point de vue de la politique .....	9
Technologie.....	9
Guichet du Parlement pour la protection de la vie privée.....	11
Sécurité nationale.....	14
L'impartition et la circulation transfrontalière des renseignements personnels.....	17
Recherche sur les nouveaux enjeux liés à la protection de la vie privée .....	19
Lois provinciales essentiellement similaires à la loi fédérale .....	21
Juridictions .....	23
Évolution de la Loi sur la protection des renseignements personnels et les documents électroniques .....	29
Modifications statutaires .....	29
Examen de la LPPDE par le Parlement en 2006 .....	30





Octobre 2005

L'honorable Peter Milliken, député  
Président  
Chambre des communes  
Ottawa

Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour la période du 1<sup>er</sup> janvier au 31 décembre 2004 conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Veuillez agréer, Monsieur, l'assurance de ma considération distinguée.

La commissaire à la protection  
de la vie privée du Canada,

Jennifer Stoddart  
Jennifer Stoddart





**Rapport annuel  
au Parlement  
2004**  
Rapport concernant  
la Loi sur la protection  
des renseignements  
personnels et les  
documents électroniques

# Vie Privée

Privacy Commissioner  
of Canada



Commissaire à la protection  
de la vie privée du Canada



Privacy Commissioner  
of Canada



Commissaire à la protection  
de la vie privée du Canada

# Privacy

## Annual Report to Parliament 2005



REPORT ON THE  
*Personal Information  
Protection and  
Electronic Documents Act*



Privacy Commissioner  
of Canada



Commissaire à la protection  
de la vie privée du Canada

# Privacy

## Annual Report to Parliament - 2005



REPORT ON THE  
*Personal Information  
Protection and  
Electronic Documents Act*

Canada



Office of the Privacy Commissioner of Canada  
112 Kent Street  
Ottawa, Ontario  
K1A 1H3

(613) 995-8210, 1-800-282-1376  
Fax (613) 947-6850  
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2006  
Cat. No. IP51-1/2005-1  
ISBN 0-662-69647-6

This publication is also available on our Web site at [www.privcom.gc.ca](http://www.privcom.gc.ca).

**Privacy Commissioner  
of Canada**

112 Kent Street  
Ottawa, Ontario  
K1A 1H3  
Tél. : (613) 995-8210  
Fax: (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca

**Commissaire à la protection  
de la vie privée du Canada**

112, rue Kent  
Ottawa (Ontario)  
K1A 1H3  
Tél. : (613) 995-8210  
Télééc. : (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca



May 2006

The Honourable Noël A. Kinsella, Senator  
The Speaker  
The Senate of Canada  
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2005.

Yours sincerely,

A handwritten signature in cursive script that reads "Jennifer Stoddart".

Jennifer Stoddart  
Privacy Commissioner of Canada



**Privacy Commissioner  
of Canada**

112 Kent Street  
Ottawa, Ontario  
K1A 1H3  
Tel.: (613) 995-8210  
Fax: (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca

**Commissaire à la protection  
de la vie privée du Canada**

112, rue Kent  
Ottawa (Ontario)  
K1A 1H3  
Tél. : (613) 995-8210  
Télec. : (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca



May 2006

The Honourable Peter Milliken, M.P.  
The Speaker  
The House of Commons  
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2005.

Yours sincerely,

A handwritten signature in dark ink that reads 'Jennifer Stoddart'.

Jennifer Stoddart  
Privacy Commissioner of Canada





# TABLE OF CONTENTS

<b>Foreword</b> .....	1
<b>Our Strengthened Mandate</b> .....	5
<b>Policy Perspective</b> .....	7
Standing on Guard for Privacy.....	7
The Year in Parliament .....	12
<b>Research into Emerging Privacy Issues</b> .....	17
<b>Substantially Similar Provincial Legislation</b> .....	19
Process for Assessing Provincial and Territorial Legislation .....	19
Substantially Similar Provincial and Territorial Legislation Enacted to Date .....	20
<b>Complaints</b> .....	23
Definitions of complaint types under <i>PIPEDA</i> .....	25
Definitions of Findings and Other Dispositions .....	27
Findings by Complaint Type.....	28
Complaint Investigations Treatment Times .....	30
Inquiries .....	32
Following Up on <i>PIPEDA</i> Case Investigations .....	33
Investigation process under <i>PIPEDA</i> .....	36

<b>Audit and Review .....</b>	<b>39</b>
Radio Frequency Identification Device (RFID) Use in Canada .....	40
RFIDs in Canada .....	41
Need for RFID Awareness and Guidance .....	42
Follow-up Audit of the Canadian Imperial Bank of Commerce .....	43
Privacy Self-assessment .....	43
<b>In the Courts .....</b>	<b>45</b>
<i>PIPEDA</i> Applications .....	45
Developments in Ongoing Applications .....	45
New Applications of Interest .....	46
Applications No Longer Proceeding .....	49
Judicial Review .....	51
<b>Public Education and Communications .....</b>	<b>53</b>
Public Opinion Research .....	54
Speeches and Special Events .....	54
Publications .....	55
Web Site .....	56
<b>Corporate Services .....</b>	<b>57</b>
Planning and Reporting .....	57
Human Resources .....	57
Finance and Administration .....	58
Information Management/Information (IM/IT) Technology .....	58
Our Resource Needs .....	59
Financial Information .....	59

## FOREWORD

**I**would like to report much good news about privacy in Canada. But it's not all good news. Concern among Canadians about their loss of privacy and the misuse of their personal information has never been greater. This concern stems from the growing threats to personal information in an electronic environment of massive and continuous data circulation.



Current private sector data protection legislation takes us only part way towards offering adequate privacy protection. The *Personal Information Protection and Electronic Documents Act (PIPEDA)* has now been in full force for two years. This law has brought Canadians outside Quebec a comprehensive suite of informational privacy rights. (Quebec adopted its own private sector privacy legislation in 1994.) It has introduced a corresponding range of obligations for organizations that collect, use and disclose personal information.

In the wake of *PIPEDA*, several provinces have moved to adopt their own legislation, which were later declared to be “substantially similar” to the standards in *PIPEDA*. British Columbia and Alberta did so in 2003, and Ontario (in health privacy matters) in 2005.

*PIPEDA* is slated for review by Parliament in 2006. This review is vital. It will present a unique opportunity to examine the Act's effectiveness in protecting one of our cherished Canadian rights, informational privacy. It will also give Parliamentarians and the Canadians they represent the chance to respond to growing attacks on personal information through identity theft, spam and fraudulent on-line activities.



Despite their limitations, *PIPEDA* and the substantially similar provincial laws have promoted a sea change in attitudes toward personal information protection in Canada. Canadians now expect organizations to justify collecting and using personal information. They are becoming increasingly vocal and articulate about the handling of their personal information.

The last few years have also created challenges for organizations covered by *PIPEDA* as they have moved, at different rates and with varying degrees of success, to implement the privacy principles of *PIPEDA*. Overall, the information handling practices brought to our attention show Canadian organizations demonstrating a high level of compliance with *PIPEDA*. Businesses, large and small, have demonstrated goodwill, commitment to community values and openness to change when it comes to protecting privacy. But I am concerned that apparent compliance does not always result in truly effective privacy and security practice. Goodwill needs to be translated into practice.

Technology, consumer trends and national security concerns continue to introduce novel uses for personal data and, indeed, require ever greater amounts of it. We must revisit how we define and apply our operating rules. How adequate are these rules in the world of the Internet, mini-computers in cars, tracking tags in clothing, satellite-assisted surveillance of neighbourhoods, and the outsourcing of data processing to countries lacking effective data protection standards? Even if we have a reliable framework for privacy protection in Canada, these protections do not always extend beyond our borders. Nor do they effectively control actions that, via the Internet, reach into Canada and use our personal information in ways that do not respect the principles of *PIPEDA*.

At the Office of the Privacy Commissioner of Canada (OPC), we continue to support privacy values through education, outreach, complaint resolution and other preventive measures. As an ombudsman, I promote voluntary compliance with privacy principles, and their adaptation to specific industry and consumer needs. I am pleased that the recent trend towards settling the privacy complaints made to my Office is continuing. Almost half of all complaints are settled to the apparent satisfaction of all parties.

As familiarity with privacy standards increases, so does the expectation that they will be observed. It is no longer acceptable that violations of personal information protection norms do not lead to direct remedial action. In 2005, I began asking organizations that are the subject of well-founded complaints to state the corrective measures they would take. I would then decide whether to seek a remedy for the

complainant in Federal Court. To date, in the few situations where I have used this approach, almost all organizations have rapidly committed to providing redress and making systemic changes.

We continue to monitor whether the systemic changes we recommended have occurred in response to complaints made in previous years. Again, the overall compliance rate is high and, once we intervene following a complaint, the level of cooperation by organizations is generally commendable.

However, it is difficult, if not impossible, to complain about misuse of personal information if individuals do not understand how their information is being used. The opaque nature of our technology-driven world means increasingly that only specialists understand the flows and uses of personal information. Because Canadians themselves may not fully understand the handling of their personal information, my Office has to rely on other indicators of privacy problems beyond those that surface through public complaints. We now use a variety of additional approaches including audit, review of information management systems, personal information assessments, public information and education to empower individuals and to help businesses with compliance, research on new issues and, where necessary, legal action.

Our mandate under *PIPEDA* is broad and demanding, and we have been hobbled by perennial uncertainty over funding. We have not had permanent funding to carry out our mandated activities under *PIPEDA*, as funding for the new law was granted initially only until 2003 and then renewed annually. *PIPEDA* has now been in full force since 2004 and the pressures are increasing. We have requested a substantial multi-year increase in our funding base and are planning for significant growth. Adequate funding will enable us to do the job our legislation requires of us. It will allow us to meet the challenge of responding to the ever-growing appetites of commercial and governmental interests for our personal information.

I would also like to commend the Honourable Gérard V. La Forest for his study on the possible merger of the offices of the Information Commissioner and the Privacy Commissioner. He concluded that a privacy-focused structure is the most appropriate framework for enforcing Canada's privacy legislation. Retaining this structure also avoids the inevitable administrative upheaval that would flow from merging the two offices. It is far better at this time that our Office continues to focus our energies on the privacy issues that we now face, and that continue to emerge, in abundance.



## OUR STRENGTHENED MANDATE

To date, our Office has not received permanent funding to carry out its duties under *PIPEDA*. Funding was granted for three years only. *PIPEDA* came into force in stages, beginning in 2001 and reaching full implementation in 2004, and we thought it important to let the dust settle before we attempted to identify long-term financial needs. *PIPEDA* has now been in full force for two years, and the demands made of us under the Act are increasing. Current funding levels leave us unable to carry out our multi-faceted mandate. For example, we face a significant backlog of complaints, and complainants are, quite understandably, becoming impatient. The small size of our team of auditors makes it impossible to conduct effective audits to ensure compliance. Even though we have adopted a risk-based approach, we need to intensify our audit activities. Funding limits also mean that our communications strategy is primarily reactive, when proactive public education about privacy rights and obligations is required instead. Similarly, our Policy and Research Branch and our Legal Services Branch are confined to putting out existing privacy fires, rather than anticipating and therefore more effectively addressing emerging privacy issues.

In the past few years, the Office went through an extremely challenging period. However, every cloud has a silver lining. In this case, the silver lining was an opportunity to review the functioning of the Office, in detail, from top to bottom. The result is an Office of the Privacy Commissioner of Canada that is pointed in the right direction. It is now time to put forward the Office's new vision and we need the full set of tools to implement it.

We are attracting new and highly specialized talent to our team. We have pursued an ambitious agenda to correct deficiencies in management of the organization. Audits and evaluations of our Office – by the Auditor General of Canada, the Public Service Commission and the Canadian Human Rights Commission – have so far been positive. And we have implemented a thoughtful, systematic process to determine

our organizational needs. This Office is now again an institution worthy of the trust of Parliament and the Canadians it serves.

## **The Vision of the Office of the Privacy Commissioner of Canada**

---

The Office has prepared two analyses of significance – a Vision and Institutional Service Plan, and a Business Case for Permanent Funding. Together, these describe who we need to be, for Canadians and on behalf of Parliamentarians, and what it takes to get us there.

If funded appropriately, the Office can accomplish the following in relation to the activities regulated under *PIPEDA*:

- undertake a meaningful number of audits and reviews to encourage greater compliance, and assist in developing a robust privacy management regime in the private sector;
- conduct legal and policy analyses of bills and legislation to assist Parliament;
- make more proactive, extensive and effective use of the enforcement tools entrusted to us by Parliament, including Commissioner-initiated complaints, court actions and public interest disclosures;
- carry out research into emerging privacy issues and trends to help citizens and policy makers understand current and future privacy challenges;
- engage in extensive public education to better inform individuals of their rights, and organizations of their obligations;
- through a streamlined investigation process, tackle the growing backlog of privacy complaints; and, finally,
- sustain institutional renewal efforts.

## **Business Case: Resources**

---

After a thorough analysis that included a Business Process Review of the investigations and inquiries functions and an in-depth review of all other functions, the Office requested a greater than 50 per cent increase in resources. The OPC is now planning for an increase within the next two years, to approximately 140 employees and an overall annual budget of approximately \$18 million.

Long-term, stable and increased funding is imperative for the OPC, for Canadians, and for the organizations covered by federal privacy laws. The OPC plans to move away from being predominately complaint-driven to a more multi-disciplinary approach, one that is more proactive than reactive, and one that better reflects the mandate given to us by Parliament.



## POLICY PERSPECTIVE

### Standing on Guard for Privacy

The focus of research and policy activity this year continued to relate to the provision of enhanced ability for law enforcement and national security agencies to obtain personal information. We reported on this extensively in the 2004-05 annual report on the *Privacy Act*, and will do so again in this coming year's annual report on that Act. The issue also merits mention here because legislation discussed or introduced in Parliament this year seeks to compel private sector organizations to release personal information.

The Commissioner appeared before the Senate Special Committee on the *Anti-terrorism Act* (ATA) on May 9, 2005. The accompanying position statement of our Office stressed the growing surveillance powers of the state as it seeks access to private sector repositories of personal data:

*Since 9/11, the Canadian government has introduced a series of measures to strengthen its surveillance powers over the citizens and residents of Canada. It also has massively invested in the development of integrated information systems that collect, process and share citizens' and residents' personal information, in a wide range of aspects of their economic and civic life: as travelers, investors, consumers, and recipients of social programs, to name a few.*

*These information systems cross organizational and jurisdictional boundaries, and redefine the parameters of time and space. Records can now be kept indefinitely, accessed through delocalized nodes, and combined and aggregated to scrutinize virtually all aspects of private life. Systems to cross-tabulate and data-mine personal information are used to categorize, sort and classify people, and to infer, deduce, and make predictive judgments on individual attitudes*

*and behaviors. Many of the systems, through the use of biometrics, delve deeply into the personal realm of identity.*

The Commissioner appeared before the House of Commons Subcommittee on the Public Safety Act and National Security on June 5, 2005, to comment on the ATA, and issued similar warnings. While many concerns related to oversight of the agencies which have special powers under the *Anti-terrorism Act*, the Office raised concerns throughout the year that *PIPEDA* was being eroded by government access to private sector databases containing personal information. We are gravely concerned that information gathered for private or commercial reasons is finding its way into government hands. This amounts to a blurring of the public and private sectors, leading to the potential use of private sector companies as agents of the state, often without the safeguards that are elemental in a democracy. We must stand on guard against state access to the databanks of the corporate world. Fears of terrorist attacks or impending pandemics provide superficially attractive justifications for intrusive powers, but the real need for these powers is often not apparent.

Some may argue that the *Privacy Act* can soften the edges of these intrusive powers. However, the Act, which governs government information collection and practices, is more than 20 years old and too antiquated and weak to provide meaningful oversight and redress for those who have been wronged. The Act was drafted even before the advent of desktop computers, let alone the myriad of other advances that enable surveillance at the push of a button.

On November 15, 2005, the Minister for Public Safety and Emergency Preparedness Canada introduced Bill C-74, *An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information*. Although the Bill died when Parliament was dissolved for the January 2006 federal election, the Bill or a variant may well be reintroduced.

The Bill would have required telecommunications service providers to establish and maintain certain capabilities to facilitate the lawful interception of information transmitted by telecommunications. The Bill would also have required telecommunications service providers to provide basic information about subscribers to the RCMP, the Canadian Security Intelligence Service (CSIS), the Commissioner of Competition and any police service constituted under the laws of a province. The legislation would have lowered the standard (at present, a warrant) that must be met to obtain disclosure of personal information. Among the main provisions of the legislation were the following:

- the requirement that all wireless, wireline, Internet and other telecommunications service providers be required to maintain existing intercept capabilities, and build in intercept capability as they upgrade their networks. Companies would be audited to ensure they are complying;
- the ability of law enforcement agencies, namely the RCMP and any police service constituted under the laws of a province, CSIS or the Commissioner of Competition, to require telecommunications service providers to surrender certain subscriber data (name, telephone number, address, e-mail address, IP address) upon request, without any judicial authorization. This would represent a change from the present situation where, under section 7(3)(c.1) of *PIPEDA*, companies are permitted to refuse requests unless they are accompanied by judicial authorization. Bill C-74 would have eliminated this discretion.

The former Bill C-74 would have also required providers to:

- enable the interception of communications generated by or transmitted through the service provider's network;
- deliver the intercepted communications to law enforcement agencies and CSIS;
- isolate or separate a communication that is authorized to be intercepted from other information/communications;
- enable simultaneous interceptions, by authorized persons from multiple national security and law enforcement agencies, of communications of multiple users. This means, for example, that a telecommunications company would have needed the capability to allow more than one agency to intercept multiple communications at the same time. The maximum capability that the Bill would have required was one intercept for every 5,000 subscribers.

Although this legislation was introduced in late 2005 and was not adopted, it is an excellent example of the growing reliance on private sector companies as "agents" of the state. Electronic surveillance of communications – "wiretapping" – is far from a new phenomenon, but what wiretaps produce in the age of electronic commerce and delivery of multiple services over the Internet is vastly greater than what flowed from tapping a telephone line. We expect that the privacy issues raised in the former Bill C-74 and any successor would preoccupy this Office and many civil liberties groups in 2006.

We also watched with interest the consultation undertaken by the Department of Finance on revising the anti-money laundering/anti-terrorist financing (AML/ATF) regime to meet international commitments. Canada is a member of the Financial Action Task Force (FATF), the international inter-governmental agency that establishes and oversees AML/ATF initiatives. In our letter to the Department, we stressed that not all countries are the same, and that Canada happens to have a well-regulated financial industry with significant privacy legislation governing financial records and institutions. We recognized the need to ensure that Canada does not become a safe haven for money launderers, but also stressed that Canada should not be expected to adopt every measure proposed by the FATF without critical scrutiny of the measure's privacy implications.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)* significantly weakens the protections provided by both *PIPEDA* and the *Privacy Act*. An individual's ability to lodge a complaint, and the Privacy Commissioner's power to investigate the complaint, are meaningless, given the secrecy surrounding the collection of personal information by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). FINTRAC's mandate is to assist in the detection, prevention and deterrence of money laundering, terrorist activity financing and/or threats to the security of Canada. The secrecy surrounding the collection of information by FINTRAC will prevent members of the public from knowing that information is being collected about them or that they are being investigated. We are seeing calls for more information to be scooped up in this net of financial surveillance, all without the knowledge of the individual, and we must protest the lack of attention to the very real privacy issues that flow from this expansion in the surveillance powers of government.

In May 2005, a multi-stakeholder task force struck by the Minister of Industry reported on a one-year study of the problem of unsolicited email, or "spam." Our Office participated on this task force, and we were gratified to see a strong commitment from the Minister to move forward rapidly to combat a pestilence that is undermining trust in the Internet and exposing hapless computer users to scams, identity theft, and even malevolent software or "spyware" that surreptitiously invades and compromises computers and the information they hold. As with many other important issues, the Office has received relatively few complaints on the use of email address information without consent. However, this is a much more significant issue than the limited number of complaints would suggest. We look forward to further government action in 2006.



Most spam originates outside Canada. This is a significant problem, since it is very difficult to investigate and prosecute the originators of spam. A similar difficulty arises with many other Internet scams, and even with legitimate businesses outside Canada collecting and processing personal information. We have struggled with this issue in a number of *PIPEDA* complaints this year. In response, we are now placing greater emphasis on harmonized international solutions and cooperation among data commissioners. In 2004, we reported on the significant concerns raised by the *USA PATRIOT Act* for the personal information of Canadians held both outside and inside Canada, and on the extensive investigation of this issue by the B.C. Information and Privacy Commissioner. Governments at both provincial and national levels need to remain alert to this and other issues related to the outsourcing of personal information.

We must all work more effectively at the international level to find solutions to the privacy issues flowing from outsourcing, just as law enforcement has attempted to address crime and money laundering internationally. Our data protection agencies simply do not have the resources (or the legal authority) to chase perpetrators on foreign soil, so it is in our interest to work towards harmonized international standards and approaches. Canada benefits enormously from outsourcing, so we are good candidates to advance solutions that work for exporters, processors and individuals. And we find it more important than ever to communicate with international bodies that focus on ways of increasing international cooperation in a number of areas. The Commissioner was invited by the Organisation for Economic Co-operation and Development (OECD) to play a significant role in trans-border cooperation, and work started in the autumn of 2005. To this end as well, the Assistant Commissioner for *PIPEDA* has attended meetings in Korea and Hong Kong this year on the Asia-Pacific Economic Cooperation (APEC) Privacy Guidelines. The participation and expertise of the Government of Canada in this exercise has clearly exerted a positive influence on the Guidelines, bringing them closer to the Canadian data protection model. The Assistant Commissioner also attended a meeting on travel documents hosted by the OECD and the International Civil Aviation Organization (ICAO) in Britain.

The Commissioner, the Director General Legal Services and the Director of Research and Policy attended the International Data Protection and Privacy Commissioners Conference in Switzerland in September 2005. Our Office will be hosting the 2007 International Data Protection and Privacy Commissioners Conference. We look forward to welcoming more than 60 data commissioners and their staff, as well as members of privacy advocacy groups and the business community, among others,



from Canada and around the world, and to working on practical ways to implement data protection measures, wherever personal data may be held. A common focus on technological issues such as biometrics, Radio Frequency Identification (RFID), standards for authentication and identity management, and surveillance devices, will hasten implementation of measures to better protect privacy and reduce costs for business.

## **The Year in Parliament**

---

The Office had a busy year in its relations with Parliament in 2005. A key component of our work involves appearing before Senate and House of Commons committees to provide expert advice on the privacy implications of bills and other policy matters under consideration by Parliament.

The Office was called on to appear before parliamentary committees 16 times this year – a considerable challenge for our small organization. Yet because the Privacy Commissioner is an Officer of Parliament, such appearances are central to her duties.

A key Committee for the Office is the relatively new Standing Committee of the House of Commons on Access to Information, Privacy and Ethics (ETHI). Established in late 2004, this Committee is significant in that with its creation, Canadians now have a standing committee of the House of Commons dedicated to privacy matters. The Privacy Commissioner of Canada and other OPC officials appeared four times before the ETHI Committee in 2005. While one reason for these appearances was to question us on the operations of our Office through examination of our Estimates and Annual Reports, MPs on the Committee also had many questions and concerns regarding some of the key privacy challenges and opportunities facing Canadians. The OPC looks forward to a continued, productive working relationship with this Committee in the 39<sup>th</sup> Parliament. As privacy issues continue to grow in number and complexity, it is vital that Parliament have a focus to examine these issues and reflect on the concerns expressed by Canadians.

The overwhelming majority of our appearances before parliamentary committees involved bills and policy issues that relate to the *Privacy Act*, but three dealt with issues relating primarily to *PIPEDA*.

✱ *Senate Study of the Financial Services Sector*

On February 16, 2005, we appeared before the Standing Senate Committee on Banking, Trade and Commerce to assist with its study of consumer issues in the Canadian financial services sector. The Senate had asked the Committee to examine the impact of federal legislation and initiatives designed to protect consumers within the financial services sector. The Committee was also asked to review the effectiveness of agencies that play a role in consumer protection and supervision of the financial services sector.

As the complaints statistics set out in this annual report show, we receive more complaints about financial institutions than about any other industry. This has been true every year since 2001, the year the first phase of *PIPEDA* came into force. However, as we advised the Senate Committee, this does not necessarily mean that financial institutions are failing to comply with *PIPEDA*. We suspect instead that it reflects the amount and the sensitivity of personal information that banks and other financial institutions are required to collect, the central role they play in our day-to-day lives, and perhaps the complexity of our relationships with these institutions.

Many complaints we receive do not flow from systemic problems. Instead, they are the result of actions by particular employees who failed to follow company policies and procedures. With complaints that we determine to be well-founded, financial institutions typically are prepared to adopt our recommendations for corrective action. As we indicated to the Senate Banking Committee, our Office generally has a very positive relationship with financial institutions.

The Senate Committee did not have the opportunity to table its final report because of the dissolution of Parliament with the federal election call. We look forward to continuing to work with the Committee on this study when the new Parliament is convened.

\* *Bill C-37 and the “Do-Not-Call List”*

On June 8, 2005, we appeared before the House of Commons Standing Committee on Industry, Natural Resources, Science and Technology to provide our views on Bill C-37, *An Act to Amend the Telecommunications Act*. The Bill enables the Canadian Radio-television and Telecommunications Commission (CRTC) to establish a national do-not-call list. It also gives the CRTC the power to levy substantial penalties against telemarketers who do not follow the rules, and to contract with a private sector third party to operate the do-not-call service. Once the list is operational, Canadians who do not wish to receive calls from companies offering goods and services will be able to add their telephone numbers to a single, centralized list that telemarketers will be required to download regularly and respect. Both the United States and the United Kingdom have similar systems.

When we appeared before the Committee, we welcomed the establishment of a do-not-call list. However, we advised that the exemptions from the list that the Committee was considering not be introduced until after consultations with Canadians. When we appeared before the Committee, the OPC had the support of some ten privacy commissioners across Canada encouraging consultation with Canadians about these exemptions – for example, exemptions for charities, pollsters or businesses that had prior relationships with the customer.

The revised Bill adopted by Parliament contained several exemptions from the do-not-call list. The revised Bill did not prohibit unsolicited telecommunications made by or on behalf of a registered charity; a registered political party; a nomination contestant, leadership contestant or candidate of a political party; or an association of members of a political party. The Bill also did not prohibit unsolicited telecommunications to a person with whom the caller has an existing business relationship and who has not made a do-not-call request to that caller, and unsolicited telecommunications made for the sole purpose of collecting information for a survey of members of the public.

Bill C-37 received Royal Assent on November 25, 2005. We are pleased with its enactment, but the exemptions unnecessarily weaken the legislation.

✱ *Bill C-57 and Financial Institutions*

On November 15, 2005, we appeared before the House of Commons Standing Committee on Finance to address Bill C-57, *An Act to amend certain Acts in relation to financial institutions*. The Bill made changes to the corporate governance framework of banks, bank holding companies, insurance companies, insurance holding companies, trust and loan companies and cooperative credit associations to bring the acts governing those institutions up to the standards adopted in 2001 for business corporations under the *Canada Business Corporations Act*. The Bill also updated certain governance standards that are unique to financial institutions.

Bill C-57 contained only a few provisions relating to the collection, use or disclosure of personal information. These included a series of provisions requiring the directors or officers of banks and other financial institutions to report any interest they may have had in a material contract or material transaction with the bank or other financial institution. Related provisions allowed shareholders to review these disclosures. C-57 also allowed shareholders to obtain personal information about other shareholders, provided that the information would be used only for the purposes specified in the Bill.

When we appeared before the Committee, we did not have any significant concerns with the Bill from a privacy perspective. We found nothing that directly affected customer information. We argued that the new emphasis on corporate governance in the proposed legislation might even enhance privacy protection because it would force corporations to become more aware of the risks of poor management practices, and it would also result in corporations placing greater emphasis on security considerations.

Bill C-57 received Royal Assent on November 25, 2005.





## RESEARCH INTO EMERGING PRIVACY ISSUES

In 2005, the OPC awarded a total of \$148,850 to five organizations through its Contributions Program for research into emerging privacy issues. This program has been part of our annual budget since 2000, but was made operational only in 2004. Studies conducted under the program delve into the thriving data brokerage industry, the use of DNA samples, workplace surveillance, and compliance with and enforcement of *PIPEDA*.

This is the second year of the program, which was launched in June 2004 to support research by not-for-profit groups, including educational institutions, industry and trade associations, and consumer, voluntary and advocacy organizations. Its goal is to further the development of a national research capacity in Canada on the broad spectrum of issues that have an impact on privacy.

The OPC is mandated to undertake and publish research related to the protection of personal information. The program was set up as part of the Office's budget pursuant to its program/legislative authority under *PIPEDA*.

Over the past two years, the Contributions Program has awarded a total of \$520,440. Research bodies across Canada are invited to apply for grants to examine various privacy issues. After a thorough screening process, the organizations are then awarded the resources to initiate the research.

The following projects were funded in 2005:

<b>Canadian Internet Policy and Public Interest Clinic</b> Ottawa, ON	<b>The PIPEDA: Compliance Testing and Special Report on the Data-Brokerage Industry</b> <i>Evaluate organizational compliance with PIPEDA and research the growing data-brokerage industry</i>	\$50,000
<b>Ryerson University</b> Toronto, ON	<b>Workplace Privacy - The Employer's Perspective</b> <i>Highlight some of the issues, concerns and interests that motivate employers in their adaptation of new workplace surveillance technology</i>	\$36,150
<b>University of British Columbia</b> Vancouver, BC	<b>A Preliminary Exploration of Workplace Privacy Issues in Canada</b> <i>Explore the challenges to privacy in the workplace posed by current and emerging technologies</i>	\$27,000
<b>British Columbia Civil Liberties Association</b> Vancouver, BC	<b>PIPEDA Enforcement Evaluation</b> <i>Comparing PIPEDA's effectiveness to similar regimes in other jurisdictions</i>	\$24,200
<b>University of Ottawa</b> Ottawa, ON	<b>Social Uses of DNA Information in the Context of Developing Policies and Analysis of two DNA related bills</b> <i>Exploration of the social uses of DNA by a comparative analysis of two DNA bills</i>	\$11,500

The projects are expected to be completed in 2006. Links to the sites where they are published will appear on the OPC's web site.

## SUBSTANTIALLY SIMILAR PROVINCIAL LEGISLATION

Section 26(2)(b) of *PIPEDA* permits the Governor in Council to issue an order exempting an organization, a class of organizations, an activity or a class of activities from the application of *PIPEDA* with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation that is substantially similar to *PIPEDA*.

The intent of this provision is to allow provinces and territories to regulate the personal information management practices of organizations operating within their borders and to promote a common standard for privacy protection throughout Canada and across sectors.

If the Governor in Council issues such an order, *PIPEDA* will not apply to the collection, use or disclosure of personal information by organizations subject to the provincial law. Personal information that flows across provincial or national borders will continue to be subject to *PIPEDA*, and the Act will continue to apply within a province to the activities of federal works, undertakings and businesses that are under federal jurisdiction – for example, banks, airlines and broadcasting and telecommunications companies.

### Process for Assessing Provincial and Territorial Legislation

Industry Canada has announced that to be substantially similar, provincial or territorial laws must:

- incorporate the ten principles in Schedule 1 of *PIPEDA*;
- provide for an independent and effective oversight and redress mechanism with powers to investigate; and

- restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.

## **Substantially Similar Provincial and Territorial Legislation Enacted to Date**

Our Office is required by section 25(1) of *PIPEDA* to report annually to Parliament on the “extent to which the provinces have enacted legislation that is substantially similar” to the Act.

In November 2003, the Governor in Council issued an Order in Council (P.C. 2003-1842, 19 November 2003) declaring Quebec’s *An Act Respecting the Protection of Personal Information in the Private Sector* substantially similar. The Act, which predated *PIPEDA*, came into effect on January 1, 1994.

British Columbia and Alberta each adopted legislation in 2003 that applies to all organizations within the two provinces, except for those covered by other provincial privacy legislation, and federal works, undertakings or businesses that remain subject to *PIPEDA*. The two laws – both called the *Personal Information Protection Act* – came into force on January 1, 2004.

The Governor in Council has issued two Orders in Council (P.C. 2004-1163, 12 October 2004 and P.C. 2004-1164, 12 October 2004) exempting organizations, other than federal works, undertakings or businesses, in Alberta and British Columbia respectively, from the application of *PIPEDA*.

Ontario’s *Personal Health Information Protection Act (PHIPA)* came into force on November 1, 2004. *PHIPA* establishes rules for the collection, use and disclosure of personal health information by health information custodians in Ontario. Health information custodians are individuals or organizations listed under *PHIPA* that, as a result of their power or duties, have custody or control of personal health information.

In September 2004, our Office informed Industry Canada that we believe *PHIPA* is substantially similar to *PIPEDA*. In November 2005, the Governor in Council issued an Order in Council (P.C. 2005-2224, 28 November 2005) exempting health information custodians in Ontario from the application of *PIPEDA*. As a result, Ontario health information custodians will not be subject to *PIPEDA* with respect to the collection, use and disclosure of personal health information. The Information and Privacy Commissioner of Ontario will be responsible for ensuring compliance

with *PHIPA*, including investigating complaints about the personal information practices of health information custodians within the province.

The Privacy Commissioner of Canada will continue to be responsible for oversight in relation to the collection, use and disclosure of personal health information that crosses provincial boundaries in the course of commercial activity. As well, our Office will continue to be responsible for personal health information collected, used or disclosed in the course of commercial activities by organizations that are not health information custodians.





# COMPLAINTS

The year 2005 was the second year in which *PIPEDA* covered all commercial activities in provinces that do not have substantially similar legislation. We saw a large drop in 2005 in the number of complaints filed under *PIPEDA*. We received 400 complaints in 2005, compared with 723 in the previous calendar year.

Complaints received between January 1 and December 31, 2005 Breakdown by Sector	Count	Percentage
Financial Institutions	113	28.25
Insurance	60	15.00
Telecommunications	55	13.75
Sales	44	11.00
Transportation	39	9.75
Accommodation	17	4.25
Professionals	13	3.25
Health	4	1.00
Services	2	0.50
Rental	1	0.25
Other	52	13.00
Total	400	100.00

We can only speculate about the reasons for fewer complaints. The volume of incoming complaints in 2004 was itself an increase over previous years, largely due to the full implementation of the Act and its coverage of new activities such as insurance, retail and accommodation, and professions such as law. The 400 complaints we received in 2005, while only 55 per cent of the number we received in 2004, were still considerably more than we received in 2001, 2002 or 2003.

We hope that the decrease in complaints indicates greater awareness by organizations of the need to comply with *PIPEDA*. That awareness would be expected to produce at least two benefits. First, organizations would bring their personal information management practices into compliance with *PIPEDA*. Second, if compliance problems arose, the organizations' privacy officers would be more conversant with *PIPEDA* and better able to resolve problems directly with individuals.

Greater awareness and understanding of *PIPEDA* may simply come with time. The reduction in complaints in 2005 was generally greater in sectors covered since the first phase of *PIPEDA* came into force in 2001. *PIPEDA* has applied since 2001 to financial institutions, telecommunications and interprovincial or international transportation. Financial institutions – which handle by far the greatest quantity of personal information – were once again the most frequent object of complaints, but the number of complaints was just over half (53 per cent) what it was in 2004. The decline was of a similar scale in the transportation (58 per cent of the total for 2004) and telecommunications (44 per cent) sectors. In the health sector, which has been covered since 2002, the decline was precipitous; we received only 11 per cent of the number of complaints we received in 2004 (although these statistics may be unreliable as indicators of trends because of the small number of complaints).

Complaints in the more recently covered sectors declined as well, except for the accommodation sector, where the number remained roughly the same as in the previous year. In the retail sector, complaint numbers were 54 per cent of the 2004 total; this may indicate a very quick uptake of *PIPEDA* principles by the retail sector. In other cases, the decline was less dramatic. The number of complaints involving insurance companies was 73 per cent of what it was in 2004, and complaints about professionals declined to 87 per cent of their previous level (although here again, the apparent trends may not be statistically significant, given the small numbers).

## Definitions of complaint types under *PIPEDA*

Complaints received in the Office are categorized according to the principles and provisions of *PIPEDA* that are alleged to have been contravened:

- **Access.** An individual has been denied access to his or her personal information by an organization, or has not received all the personal information, either because some documents or information are missing or because the organization has applied exemptions to withhold information.
- **Accountability.** An organization has failed to exercise responsibility for personal information in its possession or custody, or has failed to identify an individual responsible for overseeing its compliance with the Act.
- **Accuracy.** An organization has failed to ensure that the personal information it uses is accurate, complete, and up-to-date.
- **Challenging compliance.** An organization has failed to put procedures or policies in place that allow an individual to challenge its compliance with the Act, or has failed to follow its own procedures and policies.
- **Collection.** An organization has collected personal information that is not necessary, or has collected it by unfair or unlawful means.
- **Consent.** An organization has collected, used or disclosed personal information without valid consent, or has made the provision of a good or service conditional on individuals consenting to an unreasonable collection, use, or disclosure.
- **Correction/Notation.** The organization has failed to correct personal information as requested by an individual, or, where it disagrees with the requested correction, has not placed a notation on the information indicating the substance of the disagreement.
- **Fee.** An organization has required more than a minimal fee for providing individuals with access to their personal information.
- **Retention.** Personal information is retained longer than necessary for the fulfillment of the purposes that an organization stated when it collected the information, or, if it has been used to make a decision about an individual, has not been retained long enough to allow the individual access to the information.
- **Safeguards.** An organization has failed to protect personal information with appropriate security safeguards.

- **Time limits.** An organization has failed to provide an individual with access to his or her personal information within the time limits set out in the Act.
- **Use and disclosure.** Personal information is used or disclosed for purposes other than those for which it was collected, without the consent of the individual, and the use or disclosure without consent is not one of the permitted exceptions in the Act.

### Complaints received between January 1 and December 31, 2005

Complaint type	Count	Percentage
Use and Disclosure	143	35.75
Access	80	20.00
Collection	68	17.00
Safeguards	34	8.50
Consent	21	5.25
Time Limits	18	4.50
Accountability	10	2.50
Openness	8	2.00
Accuracy	5	1.25
Correction/Notation	5	1.25
Fee	3	0.75
Retention	3	0.75
Challenging Compliance	1	0.25
Other	1	0.25
<b>Total</b>	<b>400</b>	<b>100.00</b>

This year, the most common matter raised in complaints was the inappropriate use or disclosure of personal information. These complaints, along with those about refusal of access to personal information and inappropriate collection of personal information, comprised nearly 73 per cent of the complaints received. Last year, the picture was similar, with these categories of complaints constituting 79 per cent of the total.



## Definitions of Findings and Other Dispositions

The Office has developed a series of definitions of findings and dispositions to explain the outcome of its investigations under *PIPEDA*:

- **Not well-founded.** The investigation uncovered no or insufficient evidence to conclude that an organization violated the complainant's rights under *PIPEDA*.
- **Well-founded.** An organization failed to respect a provision of *PIPEDA*.
- **Resolved.** The investigation substantiated the allegations but, prior to the conclusion of the investigation, the organization took or committed to take corrective action to remedy the situation, to the satisfaction of our Office.
- **Well-founded and resolved.** The Commissioner, being of the view at the conclusion of the investigation that the allegations were likely supported by the evidence, before making a finding made a recommendation to the organization for corrective action to remedy the situation, which the organization took or committed to take. This finding category does not appear in the statistical tables, as it was introduced towards the end of 2005. It will appear in our statistics next year.
- **Settled during the course of the investigation.** The Office helped negotiate a solution that satisfies all involved parties during the course of the investigation. No finding is issued.
- **Discontinued.** The investigation ended before a full investigation of all the allegations. A case may be discontinued for any number of reasons – for instance, the complainant may no longer want to pursue the matter or cannot be located to provide information critical to making a finding.
- **No jurisdiction.** The investigation led to a conclusion that *PIPEDA* did not apply to the organization or activity that was the subject of the complaint.
- **Early resolution.** This applies to situations where the issue was dealt with before a formal investigation occurred. For example, if an individual filed a complaint about a type of issue that the Office had already investigated and found to comply with *PIPEDA*, we would explain this to the individual. "Early resolution" would also describe the situation where an organization, on learning of allegations against it, addressed them immediately to the satisfaction of the complainant and this Office.

Case summaries of the Commissioner's findings under *PIPEDA* are available on the OPC web site, [www.privcom.gc.ca](http://www.privcom.gc.ca).

## Findings by Complaint Type

What do complaints tell us about business organizations' compliance with *PIPEDA*? We should be cautious about reading too much into the number of complaints received, since an investigation may reveal that a complaint is not well-founded. It may be more appropriate instead to look at the findings in complaints. The chart below shows the outcome of our investigations of the different types of complaints in 2005.

### Complaints closed between January 1 and December 31, 2005

	Discontinued	Early Resolution	No Jurisdiction	Not Well-founded	Resolved	Settled	Well-founded	TOTAL
Use and Disclosure	21	6	7	31	9	52	23	149
Access	11	1	0	10	20	32	7	81
Collection	7	3	5	17	4	25	3	66
Safeguards	4	3	2	3	3	12	3	30
Consent	4	0	1	6	1	9	1	22
Accuracy	0	1	0	2	1	13	0	17
Time Limits	0	1	0	1	2	4	3	11
Correction/Notation	0	0	0	5	2	3	0	10
Accountability	1	0	0	0	3	0	0	4
Retention	1	0	0	0	1	2	0	4
Fee	0	0	0	1	1	1	0	3
Openness	0	0	0	1	0	2	0	3
Challenging Compliance	0	0	0	0	0	0	1	1
<b>TOTAL</b>	<b>49</b>	<b>15</b>	<b>15</b>	<b>77</b>	<b>47</b>	<b>157</b>	<b>41</b>	<b>401</b>

It is notable that, of 401 complaints, only 77 (19 per cent) were “not well founded.” In other words, the Commissioner could conclude that organizations had complied with *PIPEDA*'s requirements in less than one in five cases. The converse of this – the number of cases where the Commissioner could say that organizations had *not* complied with *PIPEDA*'s requirements – is more difficult to state conclusively. The number of well-founded cases is relatively small – 41, or 10 per cent – but many privacy issues are addressed by means other than full investigation, and therefore appear as “settled,” “resolved” or “early resolution.”

The significance of these numbers becomes clearer when we look at the types of complaints involved. The majority of complaints were of three types: use and disclosure (149, or 37 per cent), access (81, or 20 per cent), and collection (66, or 16 per cent). Of these, access complaints – where an individual has been denied access to his or her personal information by an organization – are the most easily remedied. A refusal by an organization to allow an individual access to personal information can be corrected by the organization granting access or by demonstrating that legitimate exceptions to the right of access apply. The ease with which access complaints can be remedied is reflected in the relatively high proportion (64 per cent) that were either settled in the course of investigation or that we considered resolved by the organization. Still, the large number of access complaints may be worrisome; it may suggest that some organizations still do not fully comprehend their responsibilities under the access provisions of *PIPEDA*. However, the number of successful resolutions is encouraging.

Complaints about inappropriate use, disclosure or collection are more troubling. These are complaints for which no simple remedy exists. If someone's personal information is inappropriately disclosed, it cannot be recalled. If someone's personal information has been inappropriately collected, the collection cannot be reversed. The Commissioner found that organizations complied with *PIPEDA*'s requirements (the complaints were "not well-founded") in only 26 per cent of the collection complaints and 21 per cent of the use and disclosure complaints.

For this reason, we intensified our focus in 2005 on maximizing the possible remedies under *PIPEDA*. We introduced a new procedure to allow the Commissioner to exert greater pressure on organizations to change their practices so that, if the damage to an individual cannot be undone, at the very least it will be less likely to happen to someone else in future. If an investigation indicates a likely contravention of *PIPEDA*, the Commissioner intervenes early, before making a finding about the complaint, with a recommendation to the organization as to how to remedy the matter. She then asks the organization to indicate within a set time how it will implement the recommendation. After receiving the organization's response, the Commissioner issues her finding.

The results of this approach have been encouraging, and it has led us to develop a new category of complaint finding, "well-founded and resolved." (This new finding category does not appear in the statistical tables, as it was introduced towards the end of 2005.) This is more than simply an exercise in rewording. It shows that organizations, almost without exception, have accepted the Commissioner's

recommendations and implemented them in a timely manner. For a person whose privacy has been irreversibly violated, this approach offers something beyond the satisfaction of knowing that the investigation supported their allegations; their complaint has led to a change; it has made a difference.

The table dealing with “complaints closed” also shows that our emphasis on settling complaints in the course of investigations continues. We commented last year that an increased focus on settlement of complaints was one way to address our complaints workload. This year, as in 2004, settlement during the course of the investigation was by far the most frequent disposition of our cases. Of the 401 complaints closed in 2005, 157 (39 per cent) were settled during the investigation. This included 38 per cent of the collection complaints and 35 per cent of the use and disclosure complaints. We will continue to seek settlements of complaints because settlement is a fundamental aspect of an ombudsman’s role, helping organizations change their cultures and sort out their problems with clients and employees.

During the year, we closed 401 complaints. This is an improvement over the previous two years, and it broke the trend of the last three years where we had received more complaints than we closed. In 2005, we closed as many complaints as we received. (A complaint received in one calendar year is not necessarily completed in that year, which is why we can close more complaints in a year than we receive.)

This has helped to reduce our complaints backlog but, like any organization that has a public complaints function, we constantly struggle to balance our resources and keep up with the influx of complaints. Some new resources will be made available in 2006 to deal with complaints, but our focus remains on finding ways to streamline procedures and process cases more effectively and efficiently.

### **Complaint Investigations Treatment Times**

---

The following tables show the average number of months taken to complete a complaint investigation, from the date the complaint is received to when a finding is made or another type of disposition occurs. The first table breaks this down by finding or disposition, the second by complaint type.



### Complaint Investigations Treatment Times for the period between January 1 and December 31, 2005, by Finding or Disposition

Finding or Disposition	Average Treatment Time in Months
Not well-founded	13.79
Resolved	13.21
Well-founded	12.44
No jurisdiction	12.27
Settled	10.17
Discontinued	7.67
Early resolution	2.53
<b>Overall average</b>	<b>10.94</b>

### Complaint Investigations Treatment Times for the period between January 1 and December 31, 2005, by Complaint Type

Complaint Type	Average Treatment Time in Months
Challenging compliance	16.0**
Collection	11.8
Accuracy	11.5
Use and disclosure	11.4
Openness	11.3*
Fee	11.0*
Access	10.9
Retention	10.8*
Consent	10.1
Accountability	10.0*
Correction/Notation	9.9
Safeguards	8.8
Time limits	6.6
<b>Overall average</b>	<b>10.9</b>

\* The treatment time for these complaint types reflects four or fewer cases each.

\*\* The treatment time for this complaint reflects one case only.



These tables of through-put times are troubling. Section 13 of *PIPEDA* requires the Commissioner to prepare her report on a complaint within one year after the filing of the complaint. As the tables show, the average time elapsed from the date of complaint to the date of finding or other disposition is just under 11 months. We might take some comfort from that, but it is uncomfortably close to the outside limit, and closer examination of the tables shows that the average time elapsed for some categories has exceeded the limit. In fact, the breakdown by finding/disposition shows that complaints that require full investigation – that is, the complaints that are “well-founded,” “not well-founded” or “resolved” – take on average more than a year to complete. (The delay in completing complaints where the finding is “no jurisdiction” reflects the complex factual and legal issues that must be addressed. Where jurisdiction is clearly not ours, the complaint does not get past our inquiries officers. If a complaint involving a jurisdictional issue has made it to the investigation phase, it is because the jurisdictional issue is not straightforward.) The length of time it is taking us to complete investigations can be attributed to a number of factors, including changes in procedures and resource issues. Whatever the reasons, it remains a matter of great concern to us, and we are focusing on ensuring that we process complaints within the period envisaged under the Act.

---

## Inquiries

The OPC’s Inquiries Unit responds to requests for information about the application of *PIPEDA* and the *Privacy Act*. The Office receives thousands of inquiries each year from the public and organizations seeking advice on private sector privacy issues.

In 2005, the Office received 5,685 inquiries related to *PIPEDA*. This was less than half the number for 2004, when we received 12,132. The total for 2004 was in turn lower than for 2003. As we noted last year, the decline may be attributable to greater understanding of *PIPEDA* among the organizations subject to it. In 2003 and 2004, on the other hand, many organizations were searching for guidance about *PIPEDA* as the Act approached full implementation on January 1, 2004.

The inquiries staff are now responding to fewer calls, but they are providing more information. An automated telephone system also helps to answer the public’s most frequently asked questions, such as those about identity theft, telemarketing and the Social Insurance Number. In addition, our web site provides a wide range of information and is increasingly used as a key resource.

## Inquiries Statistics

January 1 to December 31, 2005

### **PIPEDA Inquiries Received by the Inquiries Unit**

Telephone inquiries	4,597
Written inquiries (letter and fax)	1,088
Total number of inquiries received	5,685

### **PIPEDA Inquiries Closed by the Inquiries Unit**

Telephone inquiries	4,623
Written inquiries (letter and fax)	1,587
Total number of inquiries closed	6,210

## Following Up on PIPEDA Case Investigations

Since 2004, the Investigations and Inquiries Branch has as a matter of course monitored the progress of organizations in implementing both the commitments they make during complaint investigations and the recommendations that the Office makes to them in letters of findings. Follow-up reinforces the Office's expectations that organizations will take measures to remedy problems identified in complaint investigations. It also provides an ongoing record of organizations' compliance with PIPEDA.

The following are a few examples of actions taken by organizations as a result of our recommendations:

- An individual complained that his former employer was able to access his account with a rewards program and make changes to it. In her letter of finding, the Assistant Commissioner recommended to the organization now responsible for the rewards program that it implement password controls on the account holder information that can be accessed through its automated system. Our follow-up confirmed that the organization had introduced voice print technology and password protection for access to account holder information.

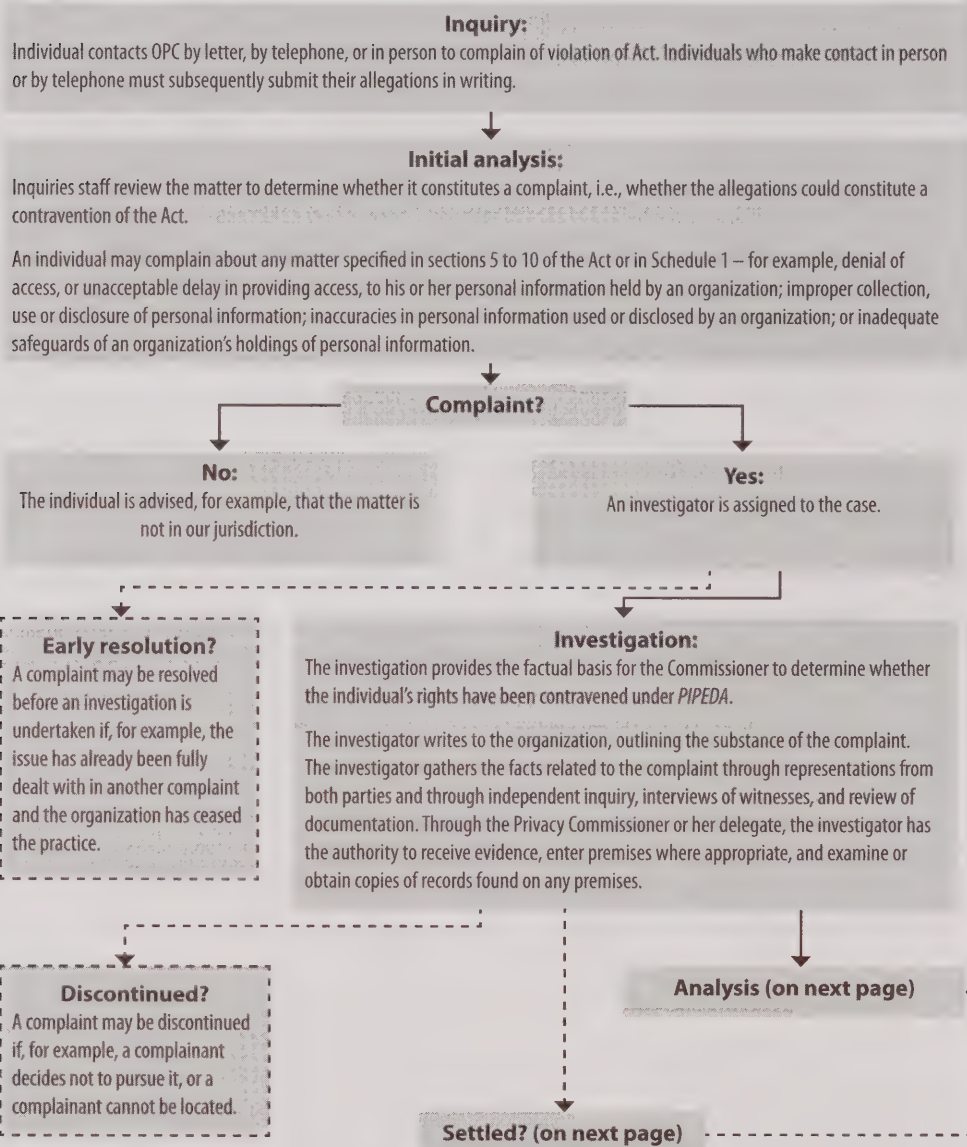
- An individual was disputing an auto insurance claim against her and sought various documents, including the claimant's statement. The insurance company refused to release the statement without the claimant's consent. The Assistant Commissioner recommended that the company sever the personal information of the third party claimant and provide the complainant with access to her personal information. She also recommended that the adjusters who work on the insurer's behalf notify third party claimants that their statements to the insurer will be shared with the insured person upon request, and that, for the purposes of providing access, only the personal information of the third party claimant that is not directly related to the statement to the insurer be severed from the statement. Our follow-up confirmed that the company did give the complainant a copy of the statement, with the relevant personal information of the claimant severed, and that the company had implemented our recommendations about its practices.
- An individual complained when his bank refused to allow him to opt-out of receiving marketing materials that were included in his credit card account statements. These materials, or "statement stuffers," were advertisements for various products and services, such as magazines or travel insurance, and were being offered by the bank in conjunction with other organizations. In response to the Assistant Commissioner's recommendations, the bank has implemented a procedure for customers to opt-out of receiving secondary marketing inserts.
- A former employee of an aviation company complained that his employer inappropriately destroyed his employment file. The Assistant Commissioner concluded that the complainant's file had been destroyed in accordance with the *Canadian Aviation Regulations*, and that the complaint was not well-founded. Nonetheless, she recommended that the company specify its maximum retention period for these files, and keep a record of when and by whom files are destroyed. Our follow-up confirmed that the aviation company amended its internal directives to specify the minimum and maximum period for retention of a pilot's file, and also instituted a log to indicate when and by whom files are destroyed.
- An individual complained that her Internet service provider failed to protect her personal information adequately, did not provide her with a satisfactory explanation when she tried to resolve her concerns, and did not give her access to the personal information she had requested. The investigation did not support the allegations about failure to protect her personal

information, and the access complaint was resolved during investigation. On the accountability issue, the Assistant Commissioner recommended that the company implement a procedure for outstanding privacy concerns to be brought to the attention of the company's privacy officer. The organization already had such a procedure, but acknowledged that its staff required greater awareness of and sensitivity to privacy. It undertook to provide the necessary training.

- An individual complained about a bank using his personal information for marketing purposes. The Assistant Commissioner concluded that the complaint was not well-founded, because the complainant had not requested that his name be suppressed from marketing lists. In reviewing the bank's privacy policy, however, she noted that it required customers to obtain and complete a form to have their names suppressed from the bank's marketing lists. She commented that this did not meet the reasonable expectations of most individuals – namely, that an immediate, easy and inexpensive means of withdrawing consent to the optional collection, use and disclosure of their personal information be provided. She therefore recommended that the bank review its opt-out procedures. In response, the bank amended its policy and procedures on direct marketing preferences. Clients wanting to opt-out of the use of their personal information for secondary marketing purposes can now simply contact any branch of the bank or the bank's call centre.



## Investigation process under *PIPEDA*



**Note:** a broken line ( - - - ) indicates a *possible* outcome.



## COMPLAINTS

### Analysis:

The investigator analyses the facts and prepares recommendations to the Privacy Commissioner or her delegate. The investigator will contact the parties and review the facts gathered during the course of the investigation. The investigator will also tell the parties what he or she will be recommending, based on the facts, to the Privacy Commissioner or her delegate. At this point, the parties may make further representations.

Analysis will include internal consultations with, for example, Legal Services or Research and Policy Branches, as appropriate.

### Findings:

The Privacy Commissioner or her delegate reviews the file and assesses the report. The Privacy Commissioner or her delegate, not the investigator, decides what the appropriate outcome should be and whether recommendations to the organization are warranted.

### Preliminary report

If the results of the investigation indicate to the Privacy Commissioner or her delegate that there likely has been a contravention of *PIPEDA*, she or her delegate recommends to the organization how to remedy the matter, and asks the organization to indicate within a set time-period how it will implement the recommendation.

The Privacy Commissioner or her delegate sends letters of findings to the parties. The letters outline the basis of the complaint, the relevant findings of fact, the analysis, and the response of the organization to any recommendations made in the preliminary report.

The possible findings are:

**Not Well-Founded:** The evidence, on balance, does not lead the Privacy Commissioner or her delegate to conclude that the complainant's rights under the Act have been contravened.

**Well-Founded:** The organization failed to respect a provision of the Act.

**Resolved:** The investigation substantiates the allegations but, prior to the conclusion of the investigation, the organization has taken or has committed to take corrective action to remedy the situation, to the satisfaction of our Office.

**Well-founded and resolved:** The investigation substantiates the allegations but the organization has taken or has committed to take corrective action to remedy the situation, as recommended in the Commissioner's preliminary report at the conclusion of the investigation.

In the letter of findings, the Privacy Commissioner or her delegate informs the complainant of his or her rights of recourse to the Federal Court.

### Settled?

The OPC seeks to resolve complaints and to prevent contraventions from recurring. The Commissioner encourages resolution through mediation, negotiation and persuasion. The investigator assists in this process.

Where recommendations have been made to an organization, OPC staff will follow up to verify that they have been implemented.

The complainant or the Privacy Commissioner may choose to apply to the Federal Court for a hearing of the matter. The Federal Court has the power to order the organization to correct its practices and to publish a notice of any action taken or proposed to correct its practices. The Court can award damages to a complainant, including damages for humiliation. There is no ceiling on the amount of damages.

**Note:** a broken line (---) indicates a *possible* outcome.



## AUDIT AND REVIEW

The goal of the Audit and Review Branch is to conduct independent and objective audits and reviews of personal information management systems for the purpose of promoting compliance with applicable legislation, policies and standards and improving privacy practices and accountability.

Section 18(1) of *PIPEDA* allows the Commissioner, after giving reasonable notice and at any reasonable time, to audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is contravening a provision of *PIPEDA*.

Given the magnitude of privacy issues and risks now facing Canadians, audit must become more central to the activities of the Office, and more proactive. We are carefully developing criteria for determining the reasonable grounds for conducting an audit. We plan to make these criteria publicly available in July 2006.

As well, as part of the upcoming review of *PIPEDA*, we are considering seeking amendments that would give the Privacy Commissioner the discretion to visit private sector entities and review their privacy management framework and practices to ensure that significant privacy risks are being identified and managed, even when a privacy breach has not become public. We believe that this discretion should also be used in particular when a significant privacy breach comes to light and the Commissioner decides that independent assurance is required that the organization concerned has taken appropriate corrective action. Such action would include critical diagnosis of internal systems and practices to remedy root causes and avoid future problems.

At the same time, we wish to support measures to encourage and help organizations to “self-regulate” and take responsibility for their own privacy governance and management. This is why, for example, we are developing a privacy self-assessment tool.

## Radio Frequency Identification Device (RFID) Use in Canada

This year, the Audit and Review Branch conducted a study of a technology that is causing considerable concern from a privacy perspective – radio frequency identification devices, or RFIDs.

RFIDs form a subset of a group of technologies, often referred to as automatic identification, that are used to help machines identify objects. An RFID “tag” can be placed in just about anything that is sold to, or used by, people. This includes bank cards, credit cards, money, passports, luggage, badges and wrist bands, clothing, vehicles and vehicle parts, appliances, phones, drugs, and food packaging. RFIDs can be implanted in livestock, and at least one company is advertising them for implanting in humans. Perhaps of greatest significance, RFIDs are capable of uniquely identifying a product.

The small size of the tags and their ability to uniquely identify an object may pose various threats to individual privacy, including the following:

- *Surreptitious collection of information.* RFID “tags” are small and can be embedded into/onto objects and documents without the knowledge of the individual who obtains those items. Tags can be read from a distance, by readers that can be incorporated invisibly into nearly any environment. Without clear notification, it may not be readily apparent that RFID technology is in use, making it virtually impossible for a person to know when or if he or she is being “scanned.”
- *Tracking an individual’s movements.* If RFID tags are embedded in clothing or vehicles, for example, and if there is a sufficiently dense network of readers in place, it becomes possible to track those tags in time and space. Applications to do just this, using a combination of RFID and Global Positioning System (GPS) technology, are being proposed by RFID vendors. If the tags can then be associated with an individual, then by that association the individual’s movements can be tracked. For example, a tag embedded in an article of clothing could serve as a *de facto* identifier for the person

wearing it. Even if information about the tagged item remains generic, identifying items people wear or carry could associate them with particular events – for example, political rallies or protests.

- *Profiling of individuals.* When using bar codes, one bottle of water has the same barcode as all other bottles of water of that particular brand. RFID technology potentially enables every object on earth to have its own unique ID (i.e., each bottle of water would have a unique identifier). There is, perhaps, the risk that the use of unique ID numbers could lead to the creation of a global item registration system in which physical objects are identified and linked to its purchaser or owner at the point of sale or transfer. If these unique identifiers are associated with an individual (by linking through a credit card number, for example), a profile of that individual's purchasing habits can easily be created.
- *Secondary use* (particularly in the sense of limiting or controlling such use). For example, the revelation of personal information such as medical prescription or personal health histories could have an impact on insurance or employment.

## RFIDs in Canada

Early in 2005 we wrote to 14 corporations in Canada asking them to help us understand the emerging use of RFIDs in Canada.

Twelve responded to the survey we sent them. The survey was not intended as a statistically representative sample of Canadian businesses as a whole. Instead, the focus was on larger corporations whose business activities were most likely to use RFID technology. The organizations included those in manufacturing, retailing, transportation, and distribution, as well as those directly involved in manufacturing RFIDs. A standard survey letter was sent to each organization asking for information about current or planned RFID use.

Of the 12 organizations that responded, two were involved in the production of RFIDs. Of the remaining ten, two were considering RFIDs, four had or would be testing RFID use, and four were using RFIDs already.

Of the four already using them, three used them to track goods, and two indicated that they linked this with personal information. One organization was using RFIDs to track employees, but stated that it was not collecting personal information.



Six of the ten organizations responded in some way to the privacy issues mentioned in the survey letter. Of the six, one indicated that it would conduct a privacy impact assessment (PIA) in reviewing the possible use of RFIDs, one would not, two others might consider a PIA or privacy compliance test in their consideration of RFIDs, and two reported that they believed a PIA was not required, since their RFID application did not identify individuals and/or link with personal information.

We learned that one central player in the RFID industry sets standards to enable and support RFID use. It also requires subscribers to respect certain privacy principles. For example, consumers must be notified of the presence of an RFID tag in an item and be given the choice to end the tag's function ("kill" the tag) after purchasing the item. As well, the tags are not to contain personal information. We are encouraged by this attention to privacy, and we call for similarly responsible practices by all those in Canada who may use RFIDs.

The only key government application for RFID of which we are now aware is its planned use in Canadian passports. We are monitoring this. As well, a group in Industry Canada is supporting and facilitating the development of commercial RFID technology.

### **Need for RFID Awareness and Guidance**

---

Even at this early stage, RFID has expanded beyond simply tracking materials. RFIDs are already being linked to personal information, and are sometimes used to track people.

Comprehensive privacy risk management for RFIDs does not yet seem to be firmly in place. Perhaps this is because RFIDs use is only beginning, with companies merely considering their business case for RFIDs, while RFID manufacturers are still focused on technical matters such as common standards to ensure security, compatibility and interoperability.

Greater public and political awareness of the potentially intrusive nature of RFID technology is essential now. The OPC will develop guidelines to help ensure that, even as RFIDs become more common, they do not erode informational privacy rights.

---

## Follow-up Audit of the Canadian Imperial Bank of Commerce

---

Between 2001 and 2004, the Canadian Imperial Bank of Commerce (CIBC) misdirected a number of facsimiles containing customers' personal information. Our Office investigated and identified concerns about privacy protection safeguards within the CIBC. In March 2005, we reported the results of this investigation to the CIBC. In light of other investigations into similar cases, we also publicly urged all banking organizations subject to *PIPEDA* to assess their policies and privacy management practices and address any shortcomings.

CIBC then reported on a number of measures to identify problems and to enhance its personal information safeguards. It also conducted an internal audit.

In a March 2005 letter to CIBC, we explained that representatives of our Audit and Review Branch would visit CIBC to verify the corrective actions that CIBC has taken and to discuss any other risks to personal information. In December 2005, we wrote CIBC that we would start this process in March 2006. We invited CIBC to send information in advance of our site visit to explain corrective actions taken by CIBC. We said that we would consider the results of the work done by the bank's internal audit department in August 2005, as well as actions taken by bank management in response.

A few weeks later, CIBC suggested meeting before our audit to confirm its scope and to understand the audit process. As requested, it agreed to give the Office a chance to examine the materials assembled in preparation for the review. We appreciate this level of cooperation. Results of our follow-up audit will appear in next year's annual report.

---

## Privacy Self-assessment

---

In our last annual report we noted that we were developing a privacy self-assessment tool for organizations to adapt and use as they wish. A draft is now being finalized with the help of internal and external expertise. The self-assessment tool is intended to promote good privacy practices and help ensure compliance with *PIPEDA*. It may also be of general interest to any entity wishing to advance privacy principles. We hope to publish the self-assessment tool in July 2006.



## IN THE COURTS

### ***PIPEDA* Applications**

**U**nder sections 14 and 15 of *PIPEDA*, a complainant or the Commissioner herself may in certain circumstances apply to the Federal Court of Canada for a hearing in respect of any matter which is referred to in the Commissioner's report and which falls within those specific clauses and sections of *PIPEDA* listed in section 14.

Since we reported on the status of ongoing court cases in our 2004 *PIPEDA* Annual Report, further developments have occurred and new applications have been filed. A selection follows of *PIPEDA* developments and new applications from 2005.

In keeping with our mandate, we have chosen not to reproduce the official style of cause in order to respect the privacy of the individual complainants. We are listing the court docket number and the name of the organization only.

### **Developments in Ongoing Applications**

#### **Telus Communications Inc.**

Federal Court Files T-1862-04, T-1863-04, T-1864-04 and T-1865-04

Federal Court of Appeal File No. A-639-05

(See 2004 *PIPEDA* Annual Report at pages 85-86.)

A hearing was held in Vancouver in September 2005. On November 29, 2005, Mr. Justice Gibson released his decision. He found that: (1) the Telecommunications Workers Union was not a proper party to the proceedings (i.e. it was not "an individual" entitled to apply to the Court); (2) the collection of the voice print

information at issue would be seen by a reasonable person to be appropriate in the circumstances pursuant to section 5(3) of the Act; and (3) Telus met its consent obligations under the Act.

The applicants filed an appeal on December 22, 2005.

#### **Alta Flights (Charters) Inc.**

Federal Court File No. T-1066-04

Federal Court of Appeal File No. A-184-05

(See our 2004 *PIPEDA* Annual Report at pages 84-85.)

The application was heard on March 15, 2005, and the decision released on March 29. The Court concluded, as had the Assistant Privacy Commissioner, that since there was no evidence that Alta Flights had recorded any conversations, the company did not actually manage to collect and/or use any personal information. In the absence of any explicit or implicit statutory language, common law principles of attempted breach cannot be read into *PIPEDA*. The Court therefore found that an attempted collection does not violate the Act.

The applicant filed an appeal of the decision in April 2005. A requisition for hearing of the appeal was filed on August 4, 2005 and the hearing date was set for March 21, 2006.

### **New Applications of Interest**

#### **Brampton Flying Club**

Federal Court File No. T-192-05

The complainant was the long-time general manager of the Brampton Flying Club (BFC) until dismissed from his position. He took legal action regarding his dismissal and also made an access request for a copy of all his personal information held by the club.

In December 2003, he complained to the Privacy Commissioner that BFC had (1) failed to provide him with his personal information within 30 days of his written request; (2) subsequently tried to charge him an unreasonable amount of \$1,500 to conduct a five-day forensic audit which BFC claimed would be necessary to answer his request; and (3) still had not supplied him with all his information.



The Assistant Commissioner determined that the statutory time limit in section 8(3) had been exceeded, that the \$1,500 charge was beyond the scope of “minimal or no cost” set out in Principle 4.9.4, and that some of the complainant’s personal information was improperly withheld by the organization.

The individual filed an application to the Federal Court under section 14 of *PIPEDA* on February 3, 2005. The Privacy Commissioner was added as a party to this application on May 18, 2005.

The Privacy Commissioner took the position that fact that the complainant may have been seeking access to documents that might assist him in parallel court proceedings between the parties was irrelevant. A complainant’s motive should not be used to limit his or her right of access to personal information under *PIPEDA*. In these unique circumstances, the Privacy Commissioner filed a confidential affidavit with the Court to identify the documents to which the complainant was seeking access and which had been withheld by the organization.

The matter was adjourned for 60 days on January 3, 2006, to allow for settlement discussions.

**Jeffrey P. Wyndowe**  
Federal Court File No. T-711-05

The complainant alleged that Dr. Wyndowe, an independent medical examiner who examined the complainant on behalf of his insurance company, refused to provide him with access to his personal information. The complainant asked for a copy of the questions the doctor asked him, as well as a record of his answers. Dr. Wyndowe refused, indicating that in his view they did not form part of the complainant’s medical record and were therefore not his personal information.

The Assistant Commissioner found that the notes taken by Dr. Wyndowe in support of his report were the complainant’s personal information as defined in section 2 of *PIPEDA*. Dr. Wyndowe then argued that the independent medical examination took place in the context of a litigious situation, and that access could therefore be denied because the information was protected by solicitor-client privilege. The Assistant Commissioner did not accept this interpretation of section 9(3)(a) of *PIPEDA*, since Dr. Wyndowe had not been retained by the insurance company as an expert in the context of ongoing litigation; rather, he was retained as an expert to help the company determine its obligations under a group insurance policy.

Nor was the Assistant Commissioner convinced that section 9(3)(d) – which permits an organization to deny access to information generated in the course of a formal dispute resolution process – could be used in this case, since processing the insurance claim did not constitute a formal dispute resolution process.

The Assistant Commissioner recommended that Dr. Wyndowe provide the complainant with access to his personal information.

The complainant filed an application to the Federal Court under section 14 of *PIPEDA* on April 25, 2005. The Privacy Commissioner was added as a party on July 7, 2005. A requisition for hearing was filed on October 3, 2005, although no date has yet been set.

### **Scotiabank**

Federal Court File No. T-2126-05

An individual complained that one or more employees of Scotiabank obtained her personal information without her consent, and that this information was then communicated to a third party.

During the investigation, it was confirmed that one of the bank's employees had improperly accessed the applicant's account profile without her consent, and had provided this information to the director of the branch, but not to any outside party. The bank had already taken disciplinary measures against this employee following its own internal investigation.

The Assistant Commissioner concluded that the bank employee had indeed violated the provisions of *PIPEDA* and that the complaint was well-founded.

The complainant filed an application to the Federal Court under section 14 of *PIPEDA* on December 1, 2005. The matter is proceeding before Federal Court.

### **Privacy Commissioner of Canada v. RBC Action Direct Inc.**

Federal Court File No. 05-T-17

An individual complained that RBC Action Direct refused to release to him all his personal information in response to an access request made under *PIPEDA*. The information included a transcript of the complainant giving instructions by telephone to an RBC Action Direct representative regarding an account which he

claimed to be a joint account between him and a third party. The organization contended that the information was the personal information only of the third party account holder, not that of the complainant, and withheld the transcript.

The Assistant Privacy Commissioner concluded that information may be personal to more than one party. In this case, there was personal information of the third-party account holder but the transcript capturing the complainant's telephone conversation with the organization's representative also constituted the personal information of the complainant. Accordingly, the complaint was well-founded and the Assistant Commissioner recommended that the organization release the transcript to the complainant. Though RBC Action Direct provided the complainant with a copy of the transcript, it severed virtually all the information in it, maintaining – despite the Commissioner's finding – that it was the account holder's personal information only.

As more than 45 days had lapsed since the issuance of the Commissioner's report, the Commissioner requested an extension of time to file a section 15(a) application in Federal Court against RBC Action Direct Inc. Leave to file the application was granted on December 16, 2005.

## Applications No Longer Proceeding

### **Canadian National Railways**

Federal Court File No. T-948-04

An individual complained that a nurse affiliated with CN shared his personal information when she revealed to his supervisor sufficient information for the supervisor to deduce that the complainant was in the company's substance abuse program, and that she disclosed further personal information about him in an email to the supervisor, superintendent and two other CN supervisors.

The Assistant Privacy Commissioner concluded that the nurse had indeed revealed too much personal information in both instances, and that the information was not necessary in the circumstances. CN therefore inappropriately used his personal information and violated Principle 4.3.

The complainant filed an application in the Federal Court under section 14 of *PIPEDA* on May 14, 2004. The Privacy Commissioner was added as a party in

October 2004 in order to make arguments concerning: (1) the scope of the Privacy Commissioner's jurisdiction and that of the Federal Court over *PIPEDA* complaints that arise in the context of a collective agreement; and (2) the proper interpretation of section 5(3) and Principle 4.3 of *PIPEDA*.

The Application was discontinued on June 8, 2005.

### **3web Corporation**

Federal Court File No. T-1603-04

(See our 2004 *PIPEDA* Annual Report at pages 88-89.)

The company discontinued the proceeding in June 2005.

### **Calm Air International Ltd.**

Federal Court File No. T-2061-04

(See our 2004 *PIPEDA* Annual Report at page 87.)

The Privacy Commissioner was added as a party on October 24, 2005. On November 18, 2005, the parties reached a settlement at mediation. The application was dismissed on January 20, 2006.

### **Citibank Canada**

Federal Court File No. T-2135-04

(See our 2004 *PIPEDA* Annual Report at page 86.)

An application under section 14 of *PIPEDA* was filed in the Federal Court on December 1, 2004. A settlement was reached at mediation. The application was dismissed on June 15, 2005.

### **King Cole Ducks Limited**

Federal Court File No. T-445-05

A Canadian Food Inspection Agency employee, working at a federally registered meat processing plant, complained that the organization was collecting personal information without consent through video cameras aimed at his workstation. The company stated that the cameras could help it address food safety concerns.

However, there was no evidence that the cameras could capture sufficiently detailed images to do this effectively. The Assistant Privacy Commissioner concluded that the organization was indeed collecting the complainant's personal information without his consent, contrary to Principle 4.3, for purposes which, upon closer examination, would not likely be considered appropriate in the circumstances pursuant to section 5(3) of *PIPEDA*.

The complainant filed an application to the Federal Court under section 14 of *PIPEDA* on March 9, 2005, requesting, among other things, an order that the organization remove the surveillance camera aimed at his workstation. This application was discontinued on November 4, 2005.

## Judicial Review

There were two applications, in accordance with section 18.1 of the *Federal Court Act*, for judicial review of the Privacy Commissioner's decisions and/or actions on the limited grounds of jurisdictional-type errors.

### **Blood Tribe Department of Health v. Privacy Commissioner of Canada et al.**

Federal Court File No. T-2222-03

Federal Court of Appeal File No. A-147-05

(See our 2004 *PIPEDA* Annual Report at pages 87-88.)

The Federal Court dismissed this judicial review application on its merits in March 2005. At that time, Mr. Justice Mosley stated that when the Privacy Commissioner is seized with a complaint over the retention and use of personal information, she has the responsibility to determine the facts and the duty to prepare a report of her findings. She cannot perform that role effectively if she is denied access to the information necessary to ascertain the facts merely because a claim of privilege is made. The Court was satisfied that the Commissioner had correctly exercised her authority to order the respondent to give her the documents in question, so that the Commissioner might herself assess the claim of solicitor-client privilege. Given the Commissioner's statutory obligation of confidentiality, such an order does not otherwise limit or deny any solicitor-client privilege that the applicant might enjoy in the documents at issue.

The applicant filed an appeal of this decision in April 2005. A requisition for hearing was filed in September 2005, but no date for a hearing has yet been set.



**Accusearch Inc., COB Abika.com**

Federal Court File No. T-2228-05

A complaint was filed against a data search and profiling organization in the United States. The Privacy Commissioner determined that, to investigate the U.S. organization, she must have the requisite legislative authority to exercise her powers outside Canada. The Commissioner concluded that *PIPEDA* cannot be construed as having extraterritorial effect. Based on available information, there were insufficient real and substantial connecting factors between the organization and Canada to deem the organization within the current scope of *PIPEDA*. In the circumstances, the applicant was informed that the Privacy Commissioner could not proceed with the complaint, as she lacked jurisdiction to compel the organization to produce evidence necessary for her to carry out an investigation and issue findings.

The applicant filed an application under section 18.1 of the *Federal Court Act* on December 19, 2005, seeking an order quashing or setting aside the Privacy Commissioner's decision that she lacks jurisdiction to investigate the complaint.

## PUBLIC EDUCATION AND COMMUNICATIONS

Section 24 of *PIPEDA* gives the Privacy Commissioner a specific mandate for public education and communications, as well as for research into privacy issues.

The Act requires the Commissioner to:

- (a) develop and conduct information programs to foster public understanding, and recognition of the purposes, of Part 1 of *PIPEDA*, which deals with personal information protection in the private sector;
- (b) undertake and publish research that is related to the protection of personal information, including any such research that is requested by the Minister of Industry;
- (c) encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 to 10; and
- (d) promote, by any means that the Commissioner considers appropriate, the purposes of Part 1.

In 2005, the OPC took several steps to gain a better understanding of Canadians' views on privacy issues, to raise awareness and understanding of privacy in general and, specifically, to help organizations understand their responsibilities, and individuals their rights, under *PIPEDA*. This has involved, for example, undertaking public opinion research, media relations activities, speeches and participation in special events and conferences, the printing and dissemination of publications, and posting information on our web site.

## Public Opinion Research

---

This year, the OPC commissioned EKOS Research Associates to conduct a public opinion study about Canadians' views on a variety of important privacy issues.

Canadians support strong and responsive public and private sector privacy laws. Approximately 70 per cent of those surveyed expressed a strong sense that their privacy and protection of their personal information were being eroded. They identified privacy as among the most important issues facing the country. That said, however, a gap remained between the perceived importance of privacy and privacy laws, and public awareness about these matters. Only one in five of those surveyed expressed "clear" awareness of privacy laws, so much education remains to be done.

There was an extremely high level of concern about cross-border sharing of personal information, and a strong demand for consent as a condition for such sharing. Approximately 90 per cent of those surveyed wished not only to be informed of such sharing, but also insisted that governments and the private sector first obtain their permission. The Government has since developed guidelines to ensure that personal information is protected when government contracts involve outsourcing – one step in the right direction.

A substantial majority of those surveyed said there was no real privacy because technology has made it too easy for governments to keep track of people. Although about three in ten were willing to allow companies to track how they shop in return for a discount on products or services, the vast majority of those surveyed wanted to be notified about the privacy implications of the products and services they buy.

## Speeches and Special Events

---

Conferences, meetings and other special events offer a unique opportunity for the OPC to reach out to its audiences and make significant contributions to the protection of personal information in Canada and abroad.

Our Office hosts a regular in-house lecture series (roughly one a month). The series features experts on a variety of privacy issues and brings together people from government, academia and other invited guests, as well as our staff.

In addition, representatives from our Office made more than fifty presentations in 2005, several focusing on *PIPEDA*. For example, in the Northwest Territories we

provided guidance on *PIPEDA*'s application to the tourism industry, and at an event in Toronto we explained *PIPEDA* to the bookkeeping industry. At a technology industry conference in Banff, we explained the importance of privacy standards.

The Privacy Commissioner and other senior officials also participated in a select number of international meetings and conferences. It is important that we participate in these meetings to establish Canada's position on privacy issues abroad and to help represent Canada's interest in strong privacy standards internationally, so that the personal information of Canadians processed in other countries is not compromised by lower privacy standards there. This has involved our Office participating in international data protection conferences, and meetings of the Asia-Pacific Economic Cooperation (APEC) and the Organisation for Economic Co-operation and Development (OECD). Our web site features some of the recent resolutions adopted by the data protection and privacy commissioners at their 2005 international conference in Montreux, Switzerland. This annual conference is an important event for the evolution of common approaches and the debate on global challenges to privacy, and we are honoured to be hosting the meeting in Montreal in 2007.

---

## Publications

Each year, the OPC produces and disseminates thousands of copies of publications to individuals and organizations seeking information on privacy matters. Increasingly, Canadians are viewing these documents on our web site. These documents include annual reports, guides for businesses and individuals about *PIPEDA*, as well as fact sheets and copies of both *PIPEDA* and the *Privacy Act*.

In 2005, we also published a new educational document – *Learning from a Decade of Experience: Quebec's Private Sector Privacy Act* – which aims to review and summarize Quebec's experience with its private sector law, which has been in force since 1994.

Quebec has had more than a decade of experience interpreting and applying its Act in numerous sectors and multiple situations. This has resulted in a rich body of jurisprudence that provides important insights for other jurisdictions dealing with private sector privacy compliance. We have heard that this publication has been extremely useful in helping to interpret *PIPEDA* and similar laws.

## Web Site

---

The OPC web site has seen a steady and significant increase in visits over the last several years. As with other organizations, our web site has become a key vehicle for sharing information with broad audiences. We are pleased to report that in 2005 we had almost a million visitors to our site – a milestone for our Office. We regularly post new material. This includes speeches, fact sheets, news releases, useful links and case summaries under *PIPEDA*. These materials give a real sense of the application of the law in a variety of circumstances.

Although public education and communications are an important part of our mandate, limited financial and human resources have constrained our ability to go much beyond simply responding to issues, rather than anticipating them and preparing public education strategies in advance. However, expected increased funding will permit more extensive public awareness initiatives and enable us to carry out a comprehensive proactive communications and outreach strategy.



## CORPORATE SERVICES

**D**uring 2005, the main priority of the Corporate Services Branch was completing the business case for stable, long-term funding. The second priority was strengthening our human resources management capacity.

### Planning and Reporting

An essential component of the institutional renewal of our Office is a strategic planning, reporting and control process. The year 2005 was our second using this new process. The strategic plan established at the beginning of the year became our road map for the year. We reviewed and made adjustments to plans and budgets throughout the year. To assist in our reporting, we continued work on our Performance Measurement Framework, and our monthly performance report system has now been in place for 18 months. This serves as a critical management tool for measuring whether our results meet our Office's targets.

### Human Resources

We continue trying to improve workplace quality and Office operations. Significant changes and improvements have been made to human resources management policies and practices.

We have implemented several human resource policies in consultation with central agencies and unions and in line with the new *Public Service Employment Act* requirements. These policies will guide us as we build on the successes of the past year and continue on our path towards renewing the Office. An Instrument of Delegation of Human Resource Management was developed and will guide managers in addressing human resource issues. A new Strategic Human Resource Plan and Staffing Strategy, as well as an Employment Equity Action Plan, will

help the OPC fulfill its mandate and ensure the recruitment of a highly qualified, diverse and representative workforce. As part of OPC's commitment to increase transparency in the staffing processes, a staff newsletter was developed; it is distributed monthly to all members of staff.

We made significant strides in organizational learning, including the development of a learning strategy with the Canada School of Public Service (CSPS), training and information sessions in values-based staffing, language training sessions, performance management, employee appraisals, and harassment awareness in the workplace. We have provided briefing sessions at our quarterly all-staff meetings and to all managers on various aspects of the new *Public Service Modernization Act* and *Public Service Employment Act*. The learning strategy and curriculum with the CSPS enables staff members to continue to develop the expertise and competencies required in their work, which in turn positions staff to assume new responsibilities and accountabilities. The learning strategy has been modified to reflect training requirements related to the new *Public Service Employment Act*.

We continue to work with the Public Service Commission and the Public Service Human Resources Management Agency of Canada on responses to recommendations in their audit reports. These include measures to allow OPC to regain its full staffing delegation authority.

## **Finance and Administration**

---

The OPC received a clean opinion on Audited 2004-2005 Financial Statements by the Office of the Auditor General of Canada. Along with the clean opinion for 2003-2004, this is a very firm indication that the Office has advanced along the path of institutional renewal. The organization has built on this success by establishing planning and review cycles, and by streamlining and improving the financial management policies and practices.

## **Information Management/Information (IM/IT) Technology**

---

The IM/IT Division has accomplished much over the past year. We have renewed our server infrastructure and increased data storage to allow for the scanning of documents. Substantial progress has been made on our information management project. Upgrades to our records management and correspondence tracking systems have been completed. Financial systems – the Salary Management System (SMS) and FreeBalance – have been upgraded, and the FreeBalance server has been upgraded as well. Five new tracking systems have been developed for the Audit and Review

Branch to allow the tracking of audit files. We have completed the Action Plan for Management of Information Technology Standards Compliance and we are working steadily towards the December 2006 compliance deadline.

## **Our Resource Needs**

---

As described earlier in this report, the Office has completed a business process review of all OPC functions. Following that review we requested a greater than 50 per cent increase in resources. We are planning for an overall budget of approximately \$18 million and 140 full-time equivalents (FTEs), and for a shift in the distribution of new resources to enable the Office to become more proactive.

## **Financial Information**

---

Past annual reports of this Office have provided financial tables relating to our expenditures. The overall financial framework in which the OPC operates is based on the government fiscal year, not on the calendar year. We are required to report on *PIPEDA* for the calendar year, whereas for the *Privacy Act*, we report on the fiscal year. For this reason, and to avoid any confusion, we have not included our Office's financial tables in this report. In any case, we set out these tables in our Reports on Plans and Priorities, as well as our Departmental Performance Reports. For additional financial information, we encourage you to visit our web site at [www.privcom.gc.ca](http://www.privcom.gc.ca).







## Gestion de l'information et technologie de l'information (GI/TI)

La Division de la GI/TI a abattu beaucoup de travail au cours de la dernière année. Nous avons renouvelé l'infrastructure du serveur et augmenté la capacité de stockage de données de façon à rendre possible le balayage de documents. Notre projet de gestion de l'information a beaucoup progressé. Nos systèmes de gestion des dossiers et de suivi de la correspondance ont été mis à niveau. Nos systèmes financiers – le système de gestion des salaires et FreeBalance – ont également été mis à niveau, tout comme le serveur de FreeBalance. Cinq nouveaux systèmes de suivi ont été mis sur pied pour la Direction de la vérification et de la revue afin que celle-ci puisse effectuer le suivi des dossiers de vérification. Nous avons finalisé le plan d'action de gestion en vue de la conformité aux normes sur la technologie de l'information, et nous poursuivons notre travail en vue de respecter le délai de décembre 2006.

## Besoins en ressources

Tel qu'établi plus tôt dans ce rapport, le Commissariat a examiné l'ensemble de ses processus opérationnels. Par suite de cet examen, nous avons demandé une augmentation de plus de 50 % de nos ressources. Nous planifions sur la base d'un budget d'environ 18 millions de dollars, d'une équipe de 140 équivalents temps plein et d'une distribution révisée des nouvelles ressources de façon à permettre au Commissariat d'être proactif.

## Information financière

Dans de précédents rapports annuels du Commissariat, nous avons présenté des tableaux financiers sur nos dépenses. Le cadre financier global encadrant les activités du Commissariat est établi selon l'année financière gouvernementale et non pas selon l'année civile. Pour la LPRPDE, les rapports sont produits par année civile, tandis que pour la *Loi sur la protection des renseignements personnels*, les rapports sont produits par année financière. Pour éviter toute confusion, nous n'incluons pas les tableaux financiers du Commissariat à ce rapport; nous les présentons dans nos rapports sur les plans et les priorités ainsi que dans nos rapports ministériels sur le rendement. Pour en savoir davantage sur l'aspect financier, prière de consulter notre site Web, à l'adresse suivante : [www.privcom.gc.ca](http://www.privcom.gc.ca).

Le Bureau du vérificateur général du Canada a émis une opinion favorable après avoir vérifié les états financiers de 2004-2005 du Commissariat, tout comme pour les états financiers de 2003-2004. Ces conclusions révèlent très clairement que le Commissariat a avancé dans la voie du renouveau organisationnel. Le Commissariat s'est appuyé sur ses réussites et a mis en place des cycles de planification et d'examen et a simplifié et amélioré ses pratiques et ses politiques de gestion financière.

## Finances et administration

et de jeter de nouveaux jalons pour le renouvellement du Commissariat. Un outil de délégation pour la gestion des ressources humaines a été élaboré et aidera les gestionnaires à composer avec les enjeux liés aux ressources humaines. Le nouveau plan stratégique des ressources humaines, la stratégie de dotation et le nouveau plan d'action pour l'équité en emploi permettront au Commissariat de réaliser son mandat et de veiller au recrutement d'employés hautement qualifiés formant un effectif diversifié et représentatif. Conformément à l'engagement du Commissariat qui vise à accroître la transparence du processus de dotation, un bulletin des employés est maintenant distribué de façon mensuelle à tout le personnel.

Nous avons grandement fait avancer l'apprentissage organisationnel; nous avons entre autres choses élaboré une stratégie d'apprentissage conjointement avec l'École de la fonction publique du Canada (EFPC), des séances de formation et d'information sur la dotation axée sur les valeurs, des séances de formation linguistique, des évaluations du rendement des employés et des séances de sensibilisation au harcèlement en milieu de travail, et nous avons mis en place une gestion du rendement. Lors des réunions trimestrielles destinées à tout le personnel et à la haute direction, nous avons présenté des séances d'information sur la *Loi sur la modernisation de la fonction publique* et la *Loi sur l'emploi dans la fonction publique*. Le programme et la stratégie d'apprentissage de l'EFPC permettent aux employés d'accroître leur savoir-faire et d'acquérir les nouvelles compétences nécessaires à leur travail, ce qui, du même souffle, permet aux employés d'assumer de nouvelles fonctions et responsabilités. La stratégie d'apprentissage a été modifiée afin qu'elle corresponde aux exigences de formation entraînées par la nouvelle *Loi sur l'emploi dans la fonction publique*.

En 2005, la grande priorité de la Direction de la gestion intégrée a été de finaliser son analyse de rentabilisation afin d'obtenir un financement stable et à long terme. En deuxième lieu, la Direction souhaitait renforcer sa capacité de gestion des ressources humaines.

## Planification et présentation de rapports

Parmi les éléments essentiels du renouveau organisationnel du Commissariat figure un processus stratégique de planification, de présentation de rapports et de contrôle. L'année 2005 a marqué la deuxième année du nouveau processus. Le plan stratégique élaboré au début de 2005 a constitué notre feuille de route pour les douze mois qui ont suivi. Nous avons également examiné et modifié nos plans et budgets tout au long de l'année. Pour faciliter la production de rapports, nous avons poursuivi notre travail sur le cadre de gestion du rendement. Notre système de rapports sur le rendement mensuel est en place depuis maintenant 18 mois; il s'avère un outil de gestion essentiel nous permettant d'établir si nos résultats correspondent aux objectifs du Commissariat.

## Ressources humaines

Nous travaillons de façon continue à une meilleure qualité du milieu de travail au Commissariat et à perfectionner nos activités. Des améliorations importantes ont ainsi été apportées aux politiques et aux pratiques de gestion des ressources humaines.

Nous avons mis en œuvre plusieurs politiques de ressources humaines en consultation avec les syndicats et les organismes centraux et conformément aux exigences de la nouvelle *Loi sur l'emploi dans la fonction publique*. Ces politiques nous permettront de poursuivre notre travail en nous appuyant sur nos réussites de l'année dernière

Les consultations du site Web du Commissariat ont augmenté de façon importante et régulière au cours des dernières années. Comme pour bien d'autres organisations, notre site Web est devenu un outil clé pour la communication d'information à un large public. Nous sommes heureux d'annoncer qu'en 2005, près d'un million de personnes ont visité notre site, ce qui représente un jalon important pour le Commissariat. Nous versions de façon périodique de nouveaux documents dans notre site, comme des discours, des fiches d'information, des communiqués, des liens utiles et des conclusions d'enquêtes réalisées en vertu de la *LPRPDE*. Ces documents donnent de l'information concrète sur l'application de la Loi dans différentes situations. Bien que les communications et la sensibilisation du grand public constituent des volets importants de notre mandat, le manque de ressources humaines et financières nous impose certaines restrictions. En effet, au lieu de prévoir les enjeux et d'élaborer des stratégies conséquentes de sensibilisation du grand public, nous avons dû réagir aux enjeux au fur et à mesure qu'ils se sont présentés. Aussi, devons-nous obtenir une augmentation de fonds afin d'entreprendre des initiatives de sensibilisation du grand public beaucoup plus vastes et de mettre en œuvre une stratégie exhaustive et proactive de communication et de rayonnement.

## Site Web

En 2005, nous avons publié un nouveau document d'information intitulé *Legons tirées de dix ans d'expérience : la Loi sur la protection des renseignements personnels dans le secteur privé* du Québec, qui fait l'examen et le résumé de l'expérience du Québec de sa loi sur la protection des renseignements personnels dans le secteur privé entrée en vigueur en 1994. Le Québec possède plus de dix ans d'expérience dans l'interprétation et l'application de sa loi, et ce, dans de nombreux secteurs et de multiples situations. Il jouit aujourd'hui d'une riche jurisprudence dont peuvent aussi s'inspirer les autres juridictions responsables d'assurer la protection des renseignements personnels dans le secteur privé. Il semble que cette publication ait été extrêmement utile pour l'interprétation de la *LPRPDE* et d'autres lois similaires.

consultent de plus en plus ces documents dans notre site Web. Parmi ces documents figurent les rapports annuels, des guides sur la *LPRPDE* à l'intention des organisations et des personnes, des fiches d'information ainsi que les lois elles-mêmes, soit la *LPRPDE* et la *Loi sur la protection des renseignements personnels*.



de contribuer de façon importante à la protection des renseignements personnels au Canada et à l'étranger.

Le Commissariat tient des conférences sur la protection de la vie privée dans ses locaux, à raison d'une fois par mois environ, avec des conférenciers experts de la protection de la vie privée provenant de différents horizons. Ces événements sont une occasion de réunir des invités du gouvernement, du milieu universitaire ou autre, ainsi que nos employés.

En 2005, des représentants du Commissariat ont fait plus de 50 présentations, dont plusieurs sur la *LPRPD*. Par exemples, dans les Territoires du Nord-Ouest, nous avons donné des orientations sur l'application de la *LPRPD* à l'industrie du tourisme; nous nous sommes rendus à Toronto pour expliquer l'importance des normes de protection de la vie privée à des organisations œuvrant dans le secteur de la comptabilité réunies pour un événement; lors d'une conférence à Banff sur l'industrie technologique, nous avons également parlé de l'importance des normes de protection de la vie privée.

La commissaire à la protection de la vie privée et d'autres représentants ont aussi participé à un certain nombre de réunions et de conférences internationales. Il

importe que nous participions à ces événements afin de communiquer à l'étranger la position canadienne sur les enjeux relatifs à la protection de la vie privée ainsi que de défendre les intérêts du Canada relativement à l'adoption de solides normes internationales de protection de la vie privée, de façon à ce que les renseignements personnels de la population canadienne qui sont traités à l'extérieur du pays ne soient pas mis en péril en raison de l'absence de normes efficaces. À cette fin, le Commissariat a participé à des conférences internationales sur la protection

des données ainsi qu'à des réunions de la Coopération économique de la zone Asie-Pacifique (APEC) et de l'Organisation de coopération et de développement économiques (OCDE). Notre site Web contient certaines des dernières résolutions

adoptées par les commissaires à la protection des données et de la vie privée lors de la conférence internationale qui s'est déroulée à Montreux (Suisse) en 2005. Cette

conférence annuelle est importante pour l'adoption d'approches communes et pour l'avancement du débat sur les défis mondiaux relatifs à la protection de la vie privée. En 2007, le Commissariat aura l'honneur d'être l'hôte de la prochaine conférence internationale, qui se tiendra à Montréal.

## Publications

Chaque année, le Commissariat produit des milliers d'exemplaires de ses publications et les diffuse auprès de personnes et d'organisations qui souhaitent s'informer sur la protection de la vie privée. Les Canadiennes et les Canadiens



## Recherche sur l'opinion publique

Cette année, le Commissariat a chargé la firme EKOS Research Associates de réaliser une étude sur l'opinion publique afin de mieux connaître les points de vue des Canadiennes et des Canadiens sur d'importantes questions relatives à la protection de la vie privée.

L'étude a révélé que la population canadienne est en faveur de lois vigoureuses et sensibles en matière de protection des renseignements personnels pour les secteurs privé et public. Environ 70 % des personnes interrogées estiment que la vie privée et la protection de leurs renseignements personnels se sont grandement dégradées et, à leur sens, la protection de la vie privée figure parmi les enjeux les plus importants auxquels le pays est confronté. Il existe néanmoins un décalage entre l'importance qu'on semble accorder à la protection de la vie privée et aux lois connexes, et la mesure dans laquelle les gens ont de véritables connaissances sur ces questions. Une personne sur cinq seulement disait saisir « clairement » ce que sont les lois sur la protection de la vie privée; aussi reste-t-il beaucoup de travail à faire pour informer les gens.

L'étude a également révélé que la population est extrêmement préoccupée par la question de l'échange transfrontalier des renseignements personnels et qu'elle souhaite vivement qu'il faille obtenir le consentement des personnes concernées avant que leurs renseignements puissent circuler. Environ 90 % des personnes interrogées ont affirmé qu'elles voulaient non seulement être informées de la circulation de leurs renseignements personnels, mais aussi que les gouvernements et le secteur privé soient tenus d'obtenir leur consentement avant de procéder à ce type d'activité. Depuis, le gouvernement a élaboré des lignes directrices de façon à protéger les renseignements personnels qu'il détient lorsqu'il a recours à l'impartition. Il s'agit d'un pas dans la bonne direction.

Une majorité importante des personnes interrogées disait croire que la vie privée n'était pas réellement protégée puisque la technologie actuelle offrait au gouvernement des moyens efficaces et (trop) faciles de faire le suivi des personnes. Environ trois personnes sur dix étaient favorables à l'idée que leurs habitudes de consommation soient suivies par des entreprises en échange de rabais sur des produits et des services, mais la vaste majorité souhaitait toutefois être avisée de l'incidence de tout achat de produit ou de service sur leurs renseignements personnels.

## Discours et événements spéciaux

Les conférences, les réunions et autres événements spéciaux sont pour le Commissariat des occasions privilégiées de s'adresser directement au grand public et

# COMMUNICATIONS ET SENSIBILISATION DU GRAND PUBLIC

En vertu de l'article 24 de la *LPRPDE*, la commissaire à la protection de la vie privée est chargée d'effectuer des activités de communication, de sensibilisation du grand public et de recherche sur des enjeux liés à la protection de la vie privée.

En vertu de la Loi, la commissaire doit :

- offrir au grand public des programmes d'information destinés à lui faire mieux comprendre la partie I de la *LPRPDE* qui traite de la protection des renseignements personnels dans le secteur privé;
- faire des recherches liées à la protection des renseignements personnels, et en publier les résultats;
- encourager les organisations à élaborer des politiques détaillées, notamment des codes de pratiques, en vue de se conformer aux articles 5 à 10;
- prend toute autre mesure indiquée pour la promotion de l'objet de la partie I de la Loi.

En 2005, le Commissariat a pris plusieurs mesures générales pour mieux comprendre les points de vue des Canadiennes et des Canadiens sur les questions de protection de la vie privée, informer la population et la sensibiliser à la protection de la vie privée. De façon plus particulière, le Commissariat a travaillé à aider les organisations à comprendre leurs responsabilités, et les personnes, leurs droits, conformément à la *LPRPDE*. À cette fin, le Commissariat a notamment effectué des recherches sur l'opinion publique, organisé des activités de relations avec les médias, prononcé des discours, participé à des conférences et à des événements spéciaux, produit et diffusé des publications et, enfin, publié de l'information dans son site Web.



que l'organisation est assujettie à la *LPRPDE*. Le demandeur a donc été informé que la commissaire à la protection de la vie privée ne pouvait pas traiter sa plainte puisqu'elle n'avait pas le pouvoir d'obliger l'organisation à présenter les preuves qui lui permettraient de faire une enquête et de rendre des conclusions.

Le 19 décembre 2005, le plaignant a fait une demande en vertu de l'article 18.1 de la *Loi sur les Cours fédérales* pour faire annuler la décision de la commissaire à la protection de la vie privée selon laquelle celle-ci n'a pas les pouvoirs nécessaires pour faire enquête.

## Révisions judiciaires

En vertu de l'article 18.1 de la *Loi sur les Cours fédérales*, deux demandes de révision judiciaire ont été présentées au sujet de décisions ou d'actions de la commissaire à la protection de la vie privée pour des motifs d'erreur juridictionnelle.

**Ministère de la Santé de la tribu des Blood c. commissaire à la protection de la**

**vie privée du Canada et al.**

N° de dossier de la Cour fédérale : T-2222-03

N° de dossier de la Cour d'appel fédérale : A-147-05

(Voir le rapport annuel de 2004 sur la *LPRPD* à la page 93.)

La Cour fédérale a rejeté la révision judiciaire sur le fond en mars 2005. Le juge Mosley avait alors affirmé que lorsque la commissaire à la protection de la vie privée est saisie d'une plainte sur la conservation et l'utilisation de renseignements personnels, elle a la responsabilité d'établir les faits et le devoir de rédiger un rapport sur ses conclusions. La commissaire ne peut toutefois pas assumer efficacement ce rôle si on lui refuse, par allégation de privilège, l'accès à l'information nécessaire. La Cour a jugé que la commissaire était en droit d'exiger de la partie intimée de lui fournir les documents dont elle avait besoin pour évaluer elle-même la demande d'invoquer le secret professionnel. Puisque la commissaire est également tenue à la confidentialité, le fait qu'elle exige les documents ne limite pas ou n'exclut pas par ailleurs la possibilité, pour la partie intimée, d'invoquer le secret professionnel par la suite.

En avril 2005, le demandeur en a appelé de la décision. Une demande d'audience a été présentée en septembre 2005, mais aucune date n'a encore été fixée.

**Accusearch Inc., COB Abika.com**

N° de dossier de la Cour fédérale : T-2228-05

Une plainte a été déposée contre une organisation de recherche de données et d'établissement de profils située aux États-Unis. La commissaire à la protection de la vie privée a déterminé que, pour effectuer une enquête auprès de cette organisation, elle devrait avoir l'autorisation légale d'exercer ses pouvoirs à l'extérieur du Canada. La commissaire a conclu que la *LPRPD* n'a aucune portée au-delà des frontières canadiennes. L'information connue n'établissait de façon ni suffisante ni concrète la présence de liens entre l'organisation et le Canada pour déterminer



**Calm Air International Ltd.**

N° de dossier de la Cour fédérale : T-2061-04

(Voir le rapport annuel de 2004 sur la *LPRPD* à la page 92.)

La commissaire à la protection de la vie privée avait été incluse dans cette affaire à titre de partie le 24 octobre 2005. Le 18 novembre 2005, les parties ont réglé leur différend par l'entremise d'un processus de médiation. La demande a été abandonnée le 20 janvier 2006.

**Citibank Canada**

N° de dossier de la Cour fédérale : T-2135-04

(Voir le rapport annuel de 2004 sur la *LPRPD* aux pages 91 et 92.)

Une demande d'audience à la Cour fédérale a été présentée le 1<sup>er</sup> décembre 2004 en vertu de l'article 14 de la *LPRPD*. Le différend a été réglé par l'entremise d'un processus de médiation. La demande a été abandonnée le 15 juin 2005.

**King Cole Ducks Limited**

N° de dossier de la Cour fédérale : T-445-05

Un employé de l'Agence canadienne d'inspection des aliments, qui travaille dans une usine de transformation de la viande enregistrée auprès du gouvernement fédéral, s'est plaint que l'organisation avait recueilli des renseignements personnels sans son consentement grâce à des caméras vidéo dirigées vers son poste de travail. L'organisation a affirmé que les caméras devaient servir à assurer la salubrité des aliments. Toutefois, aucune preuve ne démontre que les caméras peuvent enregistrer des images suffisamment détaillées pour servir efficacement à cette fin. La commissaire ajoutée à la protection de la vie privée a donc conclu que l'organisation recueillait des renseignements personnels sur le plaignant sans son consentement, ce qui contrevient au principe 4.3, et qu'elle le faisait à des fins qui, aux termes du paragraphe 5(3) de la *LPRPD*, sont susceptibles de ne pas être estimées acceptables dans les circonstances.

Le 9 mars 2005, le plaignant a demandé une audience à la Cour fédérale en vertu de l'article 14 de la *LPRPD* afin d'obtenir, entre autres choses, que l'organisation retire la caméra de surveillance dirigée vers son poste de travail. La demande a été abandonnée le 4 novembre 2005.

## Demandes abandonnées

**Compagnie des chemins de fer nationaux du Canada**  
N° de dossier de la Cour fédérale : T-948-04

Une personne s'est plainte qu'une infirmière de la Compagnie des chemins de fer nationaux du Canada (le CN) ait communiqué ses renseignements personnels et donné à son superviseur suffisamment d'information pour que celui-ci puisse déduire que le plaignant participait au programme de traitement de la toxicomanie de la compagnie. Le plaignant s'est également plaint que l'infirmière ait communiqué d'autres renseignements personnels à son sujet par courriel à son superviseur, au surintendant et à deux autres superviseurs du CN.

La commissaire adjointe à la protection de la vie privée a conclu que l'infirmière avait effectivement communiqué trop de renseignements personnels dans les deux cas et qu'il n'était pas justifié de le faire dans les circonstances. Par conséquent, le CN a indûment utilisé les renseignements personnels du plaignant et a contrevenu au principe 4.3.

Le 14 mai 2004, le plaignant a fait une demande d'audience à la Cour fédérale en vertu de l'article 14 de la *LPRPD*. La commissaire à la protection de la vie privée a été incluse dans cette affaire à titre de partie en octobre 2004 afin de présenter ses arguments sur : 1) la portée de sa juridiction et de celle de la Cour fédérale dans les cas de plaintes formulées en vertu de la *LPRPD* relativement à une convention collective; 2) l'interprétation appropriée du paragraphe 5(3) et du principe 4.3 de la *LPRPD*.

La demande a été abandonnée le 8 juin 2005.

**3web Corporation**

N° de dossier de la Cour fédérale : T-1603-04

(Voir le rapport annuel de 2004 sur la *LPRPD* à la page 94.)

L'entreprise a abandonné la plainte en juin 2005.

Le 1<sup>er</sup> décembre 2005, la plaignante a fait une demande d'audience à la Cour fédérale en vertu de l'article 14 de la *LPRPDE*. L'affaire est en traitement.

### Commissaire à la protection de la vie privée du Canada c. RBC Actions en Direct Inc.

N° de dossier de la Cour fédérale : 05-T-17

Une personne s'est plainte que la RBC Actions en Direct Inc. lui avait refusé l'accès à tous ses renseignements personnels en réponse à la demande qu'elle avait présentée en vertu de la *LPRPDE*. Parmi les renseignements demandés, le plaignant souhaitait obtenir la transcription de directives qu'il avait communiquées par téléphone à un représentant de la RBC Actions en Direct Inc. au sujet d'un compte qu'il disait être un compte conjoint qu'il avait avec un tiers. L'organisation a soutenu que les renseignements étaient ceux du tiers seulement et n'a pas communiqué la transcription.

La commissaire adjointe à la protection de la vie privée a conclu qu'un document d'information peut contenir les renseignements personnels de plus d'une personne. Dans le cas présent, l'information détenue par l'organisation contenait des renseignements personnels de la tierce partie du compte conjoint, mais la transcription de la conversation téléphonique du plaignant constitue ses renseignements personnels. Par conséquent, la plainte a été jugée fondée et la commissaire adjointe a recommandé à l'organisation de communiquer au plaignant la transcription de la conversation téléphonique. La RBC Actions en Direct Inc. a fourni la transcription au plaignant après avoir soustrait pratiquement tous les renseignements qu'elle contenait, affirmant – en dépit des conclusions de la commissaire adjointe – qu'il s'agissait des renseignements personnels du titulaire du compte seulement.

Puisque plus de 45 jours s'étaient écoulés depuis le dépôt du rapport de la commissaire, celle-ci a demandé le prolongement du délai normal afin de présenter à la Cour fédérale une demande d'audience en vertu de l'alinéa 15a) relativement à la RBC Actions en Direct Inc. L'autorisation de présenter une demande d'audience a été accordée le 16 décembre 2005.

indépendant avait eu lieu en raison d'un litige et qu'on pouvait par conséquent refuser au plaignant l'accès aux renseignements, ceux-ci étant protégés par le secret professionnel. La commissaire adjointe n'a pas admis cette interprétation de l'alinéa 9(3)(a) de la *LPRPD*, puisque la compagnie d'assurances n'avait pas fait appel au D<sup>r</sup> Wynn-dowe à titre d'expert pour le règlement du litige. En effet, le D<sup>r</sup> Wynn-dowe devait plutôt aider la compagnie à définir ses obligations selon la police d'assurance collective.

La commissaire adjointe n'a pas convenu qu'on pouvait invoquer dans ce cas-ci l'alinéa 9(3)(d), en vertu duquel une organisation peut refuser de communiquer à une personne ses renseignements personnels fournis dans le cadre du règlement officiel d'un différend. En effet, le traitement de la demande de règlement n'a pas constitué un processus de règlement formel d'un différend.

La commissaire adjointe a donc recommandé au D<sup>r</sup> Wynn-dowe de permettre au plaignant d'accéder à ses renseignements personnels.

Le 25 avril 2005, le plaignant a demandé une audience à la Cour fédérale en vertu de l'article 14 de la *LPRPD*. Le 7 juillet 2005, la commissaire à la protection de la vie privée a été incluse dans cette affaire à titre de partie. Une demande d'audience a été présentée le 3 octobre 2005, mais aucune date n'a encore été fixée.

### Banque Scotia

N° de dossier de la Cour fédérale : T-2126-05

Une personne s'est plainte qu'au moins un employé de la Banque Scotia avait obtenu des renseignements personnels la concernant sans son consentement et que ces renseignements avaient été communiqués à un tiers.

L'enquête a révélé que l'un des employés de la banque avait effectivement accédé au compte de la plaignante indûment et sans le consentement de cette dernière et qu'il avait communiqué certains renseignements au directeur de la succursale, mais pas à un tiers de l'extérieur. Au moment de l'enquête, la banque avait déjà pris des mesures disciplinaires à l'endroit de l'employé à la suite de sa propre enquête.

La commissaire adjointe a conclu que l'employé de la banque avait enfreint des dispositions de la *LPRPD* et que la plainte était fondée.



suisant sa demande écrite; 2) avait voulu lui réclamer la somme déraisonnable de 1 500 \$ pour effectuer une vérification judiciaire de cinq jours qui, de l'avis du BFC, était nécessaire pour répondre à la demande du plaignant; 3) ne lui avait toujours pas fourni tous ses renseignements personnels.

La commissaire adjointe a déterminé que le délai fixé aux termes du paragraphe 8(3) n'avait pas été respecté, que la somme de 1 500 \$ exigée ne répond pas au critère de « droits minimes » énoncé au principe 4.9.4 et que certains des renseignements personnels du plaignant avaient été indûment omis par l'organisation.

Le 3 février 2005, le plaignant a demandé une audience à la Cour fédérale en vertu de l'article 14 de la *LPRPD*. Le 18 mai 2005, la commissaire à la protection de la vie privée a été intégrée à la cause à titre de partie.

Selon la commissaire à la protection de la vie privée, le fait que le plaignant puisse avoir demandé l'accès à des documents en vue d'autres poursuites judiciaires impliquant les mêmes parties ne peut justifier le refus d'accès. Les motifs d'un plaignant ne devraient pas être invoqués pour empêcher celui-ci d'accéder à ses renseignements personnels en vertu de la *LPRPD*. Dans ces circonstances extraordinaires, la commissaire à la protection de la vie privée a déposé un affidavit auprès de la Cour afin d'indiquer les documents auxquels le plaignant souhaitait accéder et que l'organisation n'avait pas fournis.

Le 3 janvier 2006, l'affaire a été suspendue pendant 60 jours pour la tenue de discussions en vue d'un règlement.

**Jeffrey P. Wyndowe**

N° de dossier de la Cour fédérale : T-711-05

Le plaignant a allégué que le Dr Wyndowe, le médecin indépendant qui l'a examiné pour le compte de sa compagnie d'assurances, lui a refusé l'accès à ses renseignements personnels. Le plaignant a demandé une copie des questions posées par le médecin et des réponses à ces questions. Le Dr Wyndowe a refusé en affirmant qu'à son avis, ces renseignements ne faisaient pas partie du dossier médical du plaignant et qu'il ne s'agissait pas, par conséquent, de ses renseignements personnels. La commissaire adjointe a conclu que les notes prises par le Dr Wyndowe pour son rapport constituaient des renseignements personnels du plaignant en vertu de l'article 2 de la *LPRPD*. Le Dr Wyndowe a soutenu que l'examen médical



*Union* n'était pas une partie dans l'affaire (c'est-à-dire qu'il ne s'agit pas d'une « personne » autorisée à présenter une demande d'audience à la Cour); 2) la collecte de renseignements par empreinte vocale constituerait, aux termes du paragraphe 5(3) de la Loi, une collecte qu'une personne raisonnable estimerait raisonnable dans les circonstances; 3) Telus a respecté les obligations relatives au consentement imposées par la Loi.

Les demandeurs en ont appelé de la décision le 22 décembre 2005.

#### **Alta Flights (Charters) Inc.**

N° de dossier de la Cour fédérale : T-1066-04

N° de dossier de la Cour d'appel fédérale: A-184-05

(Voir le rapport annuel de 2004 sur la *LPRPDE* aux pages 89 et 90.)

La demande a été entendue le 15 mars 2005; la décision a été rendue le 29 mars. La Cour a conclu, comme l'avait auparavant conclu la commissaire adjointe, que puisque rien ne prouve que Alta Flights a enregistré des conversations, il est impossible de conclure à la collecte ou à l'utilisation de renseignements personnels par l'entreprise. En l'absence de texte légal explicite ou implicite à cet égard, on ne peut interpréter la *LPRPDE* en fonction de principes de common law relatifs à l'atteinte à la vie privée. La Cour a donc conclu qu'une tentative de collecte ne contrevient pas à la Loi.

Le demandeur en a appelé de la décision en avril 2005. Une demande d'audience a été déposée le 4 août 2005; l'audience a été fixée au 21 mars 2006.

### **Nouveaux dossiers d'intérêt**

#### **Brampton Flying Club**

N° de dossier de la Cour fédérale : T-192-05

Le plaignant assumait depuis longtemps les fonctions de directeur général pour le compte du Brampton Flying Club (BFC) au moment où il a été remercié de ses services. Par suite de son congédiement, il a entrepris des poursuites et a également fait une demande d'accès à ses renseignements personnels détenus par le BFC.

En décembre 2003, il s'est plaint à la commissaire à la protection de la vie privée que le BFC : 1) ne lui avait pas fourni ses renseignements personnels dans les 30 jours

## Demandes en vertu de la LRPPE

Conformément aux articles 14 et 15 de la LRPPE, une personne qui porte plainte, ou la commissaire elle-même, peut, dans certaines situations, demander que la Cour entende toute question dont il est fait mention dans le rapport de la commissaire et qui est visée par les articles et dispositions de la LRPPE énoncés à l'article 14.

Dans notre rapport annuel de 2004 sur la LRPPE, nous avons rendu compte de l'avancement des cas devant les tribunaux. Depuis, les dossiers ont progressé et de nouvelles demandes ont été déposées. Dans les pages qui suivent, nous présentons l'évolution des dossiers en cours et les nouvelles demandes déposées en 2005.

Conformément à notre mandat, nous avons décidé de ne pas publier l'intitulé de la cause tel qu'il apparaît officiellement pour respecter la vie privée des personnes ayant déposé une plainte. Nous ne publions que le numéro de dossier de la Cour et le nom de l'organisation.

## Dossiers en cours

**Telus Communications Inc.**

Nos de dossier de la Cour fédérale : T-1862-04, T-1863-04, T-1864-04 et T-1865-04  
N° de dossier de la Cour d'appel fédérale : A-639-05

(Voir le rapport annuel de 2004 sur la LRPPE aux pages 90 et 91.)

Une audience a eu lieu à Vancouver en septembre 2005. Le 29 novembre 2005, le juge Gibson a rendu sa décision. Il a conclu que : 1) la *Telecommunications Workers*

Dans notre dernier rapport annuel, il était indiqué que nous avions entrepris l'élaboration d'un outil d'évaluation sur la protection des renseignements personnels que les organisations allaient pouvoir utiliser et adapter à leurs besoins. Une première ébauche est en voie d'être finalisée grâce à la contribution d'experts internes et externes. L'outil vise à aider les organisations à se conformer à la *LPRPD* et à promouvoir de bonnes pratiques de gestion des renseignements personnels. Il pourra également être utile à toute entité qui souhaite approfondir ses principes de protection des renseignements personnels. Nous espérons être en mesure de rendre public le fruit de ces travaux en juillet 2006.

## Gestion des renseignements personnels : autoévaluation

seront publiés dans notre prochain rapport annuel.

direction.

Quelques semaines plus tard, la CIBC a suggéré que nous nous rencontrions avant la tenue de notre vérification afin d'en confirmer la portée et de comprendre le processus qui serait adopté. Tel que convenu, la banque a accepté de laisser le Commissariat examiner les documents pertinents en prévision de la vérification. Nous lui savons gré de sa coopération. Les résultats de notre vérification de suivi!

Dans une lettre envoyée à la CIBC en mars 2005, nous avons informé celle-ci que des représentants de la Direction de la vérification et de la revue se rendraient dans ses locaux afin de vérifier les mesures correctives prises et de discuter des autres risques potentiels à la protection des renseignements personnels. En décembre 2005, nous avons de nouveau écrit à la CIBC pour l'informer que nous entreprendrions ce processus en mars 2006. Nous avons invité la CIBC à nous envoyer de l'information avant la visite de nos représentants afin que ceux-ci soient au fait de ses mesures correctives. Nous avons indiqué que nous examinerions les résultats de sa vérification interne d'août 2005 ainsi que les mesures prises subseqüemment par sa

Nous savons également qu'un groupe d'Industrie Canada appuie actuellement le développement commercial de l'IRF.

## Nécessité de faire connaître l'IRF et d'en définir l'orientation

Bien qu'elle soit encore récente, la technologie de l'IRF est déjà utilisée à d'autres fins que le simple suivi de marchandises. En effet, l'IRF est utilisée pour établir des liens avec des renseignements personnels et parfois pour suivre le déplacement de personnes.

À l'heure actuelle, il semble qu'il n'y ait aucun cadre solide de gestion des risques à la protection des renseignements personnels pour régir l'utilisation de l'IRF. Sans doute peut-on attribuer cette situation au fait qu'il s'agit d'une technologie récente, que les entreprises sont pour l'instant davantage préoccupées par leurs analyses de rentabilisation sur l'IRF et que les fabricants de dispositifs d'IRF travaillent encore aux aspects techniques, comme la mise en place de normes de sécurité, la compatibilité et l'interopérabilité.

Il est essentiel de travailler maintenant à mieux informer le grand public et les intervenants politiques sur le danger que pose la nature envahissante de l'IRF. Le Commissariat élaborera des lignes directrices de façon à ce que le jour où l'IRF fera partie de notre quotidien, notre droit à la vie privée sera protégé.

## Vérification de suivi de la Banque Canadienne Impériale de Commerce

De 2001 à 2004, la Banque Canadienne Impériale de Commerce (CIBC) a mal achevé un certain nombre de télécopies contenant les renseignements personnels de clients. Le Commissariat a mené une enquête et détecté des problèmes sur le plan des mesures visant à assurer la protection des renseignements personnels à la CIBC. En mars 2005, nous avons communiqué les résultats de notre enquête à la CIBC. Puisque d'autres enquêtes du genre ont eu lieu, nous avons vivement et publiquement exhorté toutes les organisations bancaires visées par la *LPRPD* à examiner leurs politiques et leurs pratiques de gestion des renseignements personnels et à remédier à toute lacune détectée.

La CIBC a ensuite présenté un certain nombre de mesures visant à détecter les problèmes et à améliorer ses mesures de protection des renseignements personnels des clients. Elle a également procédé à une vérification interne.

organisations participantes faisaient partie des industries de la fabrication, du commerce de détail, du transport, de la distribution ainsi que de la fabrication de dispositifs d'IRF. Chaque organisation a donc reçu une lettre pour solliciter de l'information sur l'utilisation actuelle ou à venir de l'IRF.

Des douze organisations ayant répondu, deux effectuaient des activités liées à la production d'IRF. Parmi les dix autres organisations, deux envisageaient de recourir à la technologie d'IRF, quatre s'en servaient déjà; les quatre autres s'approprièrent à l'essayer ou l'avaient déjà fait.

Parmi les quatre organisations utilisant déjà la technologie d'IRF, trois s'en servent pour faire le suivi de marchandises, deux s'en servent pour établir des liens avec des renseignements personnels. Une organisation a indiqué qu'elle recourait à cette technologie pour faire le suivi de ses employés sans toutefois recueillir de renseignements personnels.

Six des dix organisations ont fourni des indications relativement aux questions sur la protection de la vie privée contenues dans notre lettre. L'une d'elles a indiqué qu'elle effectuerait une Évaluation des facteurs relatifs à la vie privée (ÉFVP) pour examiner la possibilité d'utiliser l'IRF; une autre a indiqué qu'elle ne ferait pas cette évaluation; deux autres ont indiqué qu'elles envisageraient la possibilité d'effectuer soit une EFVP, soit un autre type d'évaluation pour vérifier la conformité aux principes de protection de la vie privée; enfin, deux organisations ont affirmé qu'une EFVP n'était pas nécessaire puisqu'elles n'utilisaient pas l'IRF pour identifier des personnes ou établir des liens avec les renseignements personnels de personnes.

Nous avons appris l'existence d'une organisation centrale qui, dans l'industrie de l'IRF, définit les normes applicables à l'utilisation de l'IRF. Cette organisation exige également de ses abonnés qu'ils respectent certains principes de protection des renseignements personnels. Par exemple, les consommateurs doivent être informés de la présence d'un dispositif d'IRF lorsqu'ils achètent un article; ils doivent aussi pouvoir rendre le dispositif inopérant après l'achat. De plus, les dispositifs ne doivent pas contenir de renseignements personnels. Pour nous, l'attention accordée à la protection de la vie privée est un signe positif; nous encourageons donc toute organisation canadienne qui a recours à l'IRF à adopter des pratiques responsables similaires.

À ce jour, il semble que la seule utilisation que le gouvernement prévoit faire de l'IRF a trait aux passeports canadiens. Nous surveillons de près l'évolution de ce dossier.



suffisamment dense en place, il devient possible d'effectuer le suivi des dispositifs dans le temps et dans l'espace. Certains vendeurs proposent des applications précisément conçues à cette fin, des applications qui combinent la technologie de l'IRF et celle du système mondial de localisation (GPS). Ensuite, si on associe un dispositif donné à une personne, on peut suivre les déplacements de celle-ci. Par exemple, un dispositif intégré à un vêtement peut servir à identifier la personne qui le porte. Même si l'information sur l'article comportant le dispositif demeure somme toute générale, elle peut servir à associer des personnes à certains événements, comme des rassemblements politiques ou des manifestations.

- *Etablissement du profil des consommateurs.* Avec les codes à barres, les bouteilles d'eau d'une même marque ont toutes le même code. La technologie de l'IRF permet, pour sa part, d'attribuer un code d'identification unique à chacun des objets de la planète. (Ainsi, les bouteilles d'eau, même d'une même marque, peuvent toutes avoir leur propre code.) Il pourrait donc s'ensuivre la création d'un système d'enregistrement mondial par lequel chaque objet existant serait codé et permettrait d'associer son acheteur ou son propriétaire au lieu de vente ou de transfert. Ces liens entre une personne et les objets qu'elle acquiert (liens effectués grâce à un numéro de carte de crédit, par exemple) permettent de dresser facilement le profil de consommation d'une personne.

- *Utilisation secondaire* (en particulier en ce qui concerne le contrôle et la restriction de l'utilisation secondaire des renseignements). Par exemple, la communication de renseignements personnels comme les médicaments prescrits à une personne ou ses antécédents médicaux peuvent avoir des conséquences sur son admissibilité à une assurance ou sur ses possibilités d'emploi.

## L'identification par radiofréquence au Canada

Au début de 2005, nous avons écrit à 14 organisations canadiennes pour leur demander de nous aider à mieux comprendre l'utilisation de plus en plus fréquente de l'IRF au Canada.

Douze organisations ont accepté de participer à notre étude, laquelle ne se voulait pas nécessairement représentative de l'ensemble des entreprises canadiennes. Il s'agissait plutôt d'une étude sur les sociétés de grande envergure dont les activités commerciales sont susceptibles de faire appel à l'utilisation de l'IRF. Les

la commissaire juge qu'il doit y avoir une assurance indépendante que l'organisation concernée prend les mesures correctives appropriées. Dans le cadre de la vérification, un diagnostic serait posé sur les pratiques et systèmes internes pour combattre les problèmes à la source et en éviter d'autres.

Parallèlement, nous favorisons la prise de mesures qui encouragent et aident les organisations à s'autoréglementer et à assumer les responsabilités qui leur incombent en vue d'assurer leur propre gouvernance et leur propre gestion de la protection de la vie privée. C'est pour cette raison, notamment, que nous travaillons à l'élaboration d'un outil d'autoévaluation de la protection de la vie privée.

## L'utilisation de dispositifs d'identification par radiofréquence au Canada

Cette année, la Direction de la vérification et de la revue a effectué une étude sur une technologie suscitant d'importantes préoccupations dans le domaine de la vie privée : l'identification par radiofréquence (IRF).

L'IRF appartient aux technologies dites d'identification automatique utilisées pour permettre à des appareils de détecter des objets. Les dispositifs d'IRF peuvent être intégrés à presque n'importe quel article de vente ou objet, y compris les cartes bancaires, les cartes de crédit, les billets de banque, les passeports, les bagages, les insignes et les bracelets, les vêtements, les véhicules, les pièces de véhicule, les appareils électroménagers, les téléphones, les médicaments et les emballages alimentaires. Les dispositifs d'IRF peuvent aussi être implantés à des animaux d'élevage, et au moins une entreprise fait de la publicité pour l'implant humain. L'une des principales caractéristiques de l'IRF est sans doute que celle-ci permet d'identifier de façon unique chaque produit ou objet. Cette caractéristique, ainsi que la petite taille des dispositifs, peuvent toutefois être la source de menaces à la vie privée, par exemple :

- *Collecte subreptice de renseignements.* Les dispositifs d'IRF sont minuscules et peuvent être fixés ou intégrés à des objets et à des documents à l'insu des personnes qui les acquièrent. Les dispositifs peuvent être lus à distance par des lecteurs invisibles intégrés à presque n'importe quel milieu. Ainsi, sans avis clair à ce sujet, le recours à la technologie d'IRF peut passer inaperçu. Les consommateurs n'ont alors pratiquement aucun moyen de savoir s'ils sont « scannés » et à quel moment ils le sont.

- *Suivi des déplacements de personnes.* Si des dispositifs d'IRF sont fixés à des vêtements ou à des véhicules, par exemple, et s'il y a un réseau de lecteurs

7 L'objectif de la Direction de la vérification et de la revue est de procéder de façon objective et indépendante à la vérification et à l'examen de systèmes de gestion des renseignements personnels dans le but de promouvoir la conformité aux lois, aux politiques et aux normes en vigueur ainsi que d'améliorer les pratiques en matière de protection de la vie privée et de reddition de comptes.

Conformément au paragraphe 18(1) de la *LPRPDE*, la commissaire peut, sur préavis suffisant et à toute heure convenable, procéder à la vérification des pratiques de l'organisation en matière de gestion des renseignements personnels si elle a des motifs raisonnables de croire que cette organisation a contrevenu à l'une des dispositions de la *LPRPDE*.

En raison de l'ampleur des enjeux et des risques à la protection de la vie privée avec lesquels les Canadiennes et les Canadiens doivent composer, les activités de vérification doivent être davantage au cœur du travail du Commissariat ; celui-ci doit adopter des façons de faire plus proactives. Nous nous sommes attelés à l'élaboration minutieuse des critères définissant les motifs raisonnables qui justifient la tenue d'une vérification. Nous prévoyons être en mesure de rendre publics ces critères en juillet 2006.

En outre, en prévision de l'examen imminent de la *LPRPDE*, nous songeons à proposer des modifications qui donneraient à la commissaire à la protection de la vie privée le pouvoir discrétionnaire nécessaire de rendre visite à des organisations du secteur privé et d'examiner leurs pratiques et leur cadre de gestion de la protection de la vie privée. Cet examen permettrait de voir si les risques importants en matière de protection de la vie privée peuvent être détectés et gérés, même lorsqu'un problème donné n'est pas du domaine public. Ce pouvoir devrait aussi être exercé lorsqu'un problème important d'atteinte à la vie privée est révélé et que



L'enquêteur analyse les faits et formule ses recommandations à l'intention de la commissaire à la protection de la vie privée ou de sa déléguée. Il informe également les parties des recommandations fondées sur l'analyse des faits qu'il remettra à la commissaire ou à sa déléguée. À cette étape, les parties peuvent faire d'autres auditions d'arguments.

Au besoin, des consultations internes sont effectuées avec, par exemple, le concours de la Division des services juridiques ou de la Direction de la recherche et des politiques.

### Analyse

### Conclusions

La commissaire à la protection de la vie privée ou sa déléguée examine le dossier et évalue le rapport. La commissaire ou sa déléguée, et non l'enquêteur, détermine les conclusions à tirer et décide s'il faut présenter des recommandations à l'organisation.

### Rapport préliminaire

Si les résultats de l'enquête permettent de conclure qu'il y avait selon toute probabilité infraction à la *LRPDC*, la commissaire à la protection de la vie privée ou sa déléguée recommande à l'organisation des mesures pour remédier au problème et lui demande de lui indiquer dans un délai précis comment elle entend mettre ces mesures en œuvre.

La commissaire ou sa déléguée envoie la lettre de conclusions d'enquêtes aux parties. Cette lettre présente la plainte, les faits établis, l'analyse et la réponse de l'organisation à toute recommandation faite dans le cadre du rapport préliminaire.

Les conclusions possibles sont les suivantes :

**Non fondée :** La preuve ne permet pas à la commissaire à la protection de la vie privée ou à sa déléguée de conclure que le droit à la protection de la vie privée du plaignant en vertu de la *LRPDC* a été enfreint.

**Fondée :** L'organisation n'a pas respecté l'une des dispositions de la Loi.

**Résolue :** La preuve recueillie au cours de l'enquête donne raison au plaignant mais, avant que l'enquête ne soit terminée, l'organisation prend ou s'engage à prendre des mesures pour corriger le problème.

**Fondée et résolue :** L'enquête donne raison au plaignant, et l'organisation prend ou s'engage à prendre les mesures correctives recommandées dans le rapport préliminaire de la commissaire, au terme de l'enquête.

Dans la lettre de conclusions, la commissaire à la protection de la vie privée ou sa déléguée informe le plaignant de son droit de recours devant la Cour fédérale.

Lorsque des recommandations sont présentées à une organisation, des employés du Commissariat effectuent un suivi pour vérifier si elles ont bel et bien été appliquées.

Le plaignant ou la commissaire à la protection de la vie privée peut choisir de demander une audience devant la Cour fédérale. La Cour fédérale a le pouvoir d'ordonner à une organisation de corriger ses pratiques ainsi que de publier un avis énonçant les mesures prises ou envisagées pour corriger ses pratiques. La Cour peut accorder des dommages et intérêts au plaignant, notamment en réparation de l'humiliation subie. Il n'existe pas de plafond pour ces dommages-intérêts.

Note : une ligne discontinue (---) indique un résultat possible.



# Processus d'enquête en vertu de la LPRPD

## Demande de renseignements

Une personne qui croit que la Loi a été enfreinte communique avec le Commissariat par téléphone, par lettre ou en personne. Si la personne décide de communiquer avec le Commissariat par téléphone ou en personne, elle devra ensuite présenter ses allégations par écrit.

## Analyse initiale

Le personnel des demandes de renseignements examine le dossier afin d'établir s'il s'agit d'une plainte, c'est-à-dire si la Loi a été enfreinte. Une personne peut déposer une plainte aux termes des articles 5 à 10 ou de l'annexe I de la Loi. Par exemple, une plainte peut porter sur : 1) le refus, par une organisation, de fournir à une personne ses renseignements personnels ou de les lui fournir dans les délais prescrits par la Loi; 2) la collecte, l'utilisation ou la communication inappropriée de renseignements personnels; 3) l'utilisation ou la communication de renseignements inexacts au sujet d'une personne; 4) l'absence de mesures de sécurité pour assurer la protection des renseignements personnels détenus par une organisation; etc.

## Plainte ?

## Acceptée

La personne est avisée, par exemple, que la demande ne relève pas de notre juridiction.

Un enquêteur est chargé de l'affaire.

## Règlement rapide ?

Une plainte peut être résolue avant le début de l'enquête; par exemple, le problème peut avoir fait l'objet d'une plainte antérieure et, depuis, l'organisation concernée a mis fin à la pratique problématique.

## Enquête

L'enquête permet d'établir les faits; la commissaire détermine ensuite si le droit à la protection de la vie privée du plaignant en vertu de la LPRPD a été enfreint. L'enquêteur écrit à l'organisation pour lui présenter l'objet de la plainte. Il établit les faits grâce à l'audition d'arguments des deux parties, à la tenue d'une enquête indépendante, à l'interrogation des témoins et à l'examen de la documentation. L'enquêteur peut, de par ses pouvoirs conférés par la commissaire ou par sa déléguée, recevoir des éléments de preuve, visiter les locaux de l'organisation au besoin et examiner ou se faire remettre des copies de documents trouvés dans les locaux visités.

## Analyse (suite)

## ?

Il est possible qu'une plainte soit abandonnée dans des cas où, par exemple, la personne qui s'est plainte décide d'abandonner l'affaire ou est impossible à trouver.

## Plainte résolue ? (suite)

Note : une ligne discontinue (---) indique un résultat possible.

et de quelle manière. Notre suivi a permis de confirmer que la compagnie aérienne a modifié ses directives internes, qu'elle fixe désormais des périodes minimales et maximales de conservation des dossiers de pilote et qu'elle a instauré un système de suivi de la destruction des dossiers.

- Une personne se plaint que son fournisseur de services Internet ne protège pas ses renseignements personnels de façon adéquate, qu'il ne lui fournit pas d'explication satisfaisante en réponse à ses préoccupations et qu'il lui refuse l'accès à ses renseignements personnels. L'enquête a permis de conclure que les allégations relatives à la protection des renseignements personnels sont non fondées. Quant à la question de l'accès, celle-ci est réglée en cours d'enquête. Pour ce qui est des responsabilités du fournisseur, la commissaire a recommandé à ce dernier de mettre en œuvre une procédure selon laquelle les problèmes relatifs à la protection des renseignements personnels sont transmis à l'agent de la protection de la vie privée de l'organisation. L'organisation avait déjà une telle procédure mais a reconnu qu'elle devait sensibiliser et mieux informer ses employés quant aux questions de protection des renseignements personnels. L'organisation s'est engagée à offrir la formation requise.

- Une personne se plaint qu'une banque utilise ses renseignements personnels à des fins de marketing. La commissaire adjointe conclut que la plainte est non fondée puisque le plaignant n'avait pas demandé que son nom soit éliminé des listes de marketing. Elle note toutefois que selon la politique de la banque, les clients doivent obtenir et remplir un formulaire afin que leur nom soit retiré des listes de marketing. Selon la commissaire adjointe, cette procédure ne répond pas aux critères qui définissent une « attente raisonnable pour la plupart des personnes »; la procédure devrait permettre l'accès à un moyen immédiat, facile et peu coûteux de retirer son consentement à la collecte, à l'utilisation et à la communication de renseignements personnels. Par conséquent, la commissaire adjointe recommande que la banque revoise sa procédure relative à l'option de refus. Cette dernière a donc modifié sa politique et ses procédures de marketing direct. Désormais, les clients qui souhaitent que leurs renseignements personnels ne soient pas utilisés à des fins de marketing secondaire peuvent appeler n'importe laquelle des succursales de la banque ou encore son centre d'appels.

- l'organisation désormais responsable du programme de récompenses de mettre en place des mots de passe pour contrôler l'accès, dans son système automatisé, aux renseignements des titulaires de comptes. Notre suivi a permis de confirmer que l'organisation avait mis en place une technologie d'empreinte vocale ainsi que des mots de passe pour protéger l'accès aux renseignements des titulaires de comptes.
- Une personne conteste une demande de règlement d'assurance automobile qui la vise et demande à obtenir différents documents, dont la déclaration du demandeur. La compagnie d'assurance refuse de communiquer la déclaration sans le consentement de son auteur. La commissaire adjointe recommande à la compagnie de biffer ou de retirer les renseignements personnels de l'auteur de la déclaration et de fournir à la personne qui se plaint l'accès aux renseignements personnels qui la concernent. Elle recommande également que les experts qui travaillent pour le compte de la compagnie d'assurance informent les tiers que leur déclaration sera communiquée à la personne visée si celle-ci le demande et que seuls les renseignements personnels qui ne sont pas directement liés à la déclaration seront biffés ou retirés. Notre suivi a permis de confirmer que la compagnie a donné à la personne qui s'est plainte une copie de la déclaration de laquelle on avait supprimé les renseignements personnels du demandeur, et que la compagnie avait modifié ses pratiques conformément à nos recommandations.
- Une personne se plaint que la banque ne lui donne pas l'option de refuser de recevoir la publicité accompagnant ses relevés de carte de crédit. Les « circulaires » jointes aux relevés visent à faire connaître différents produits et services, comme des magazines ou de l'assurance voyage; elles sont offertes par la banque conjointement avec d'autres organisations. Par suite des recommandations de la commissaire adjointe, la banque a adopté une procédure qui permet à ses clients de refuser que de la publicité leur soit envoyée.
- Un ancien employé d'une compagnie aérienne se plaint que son employeur a indûment détruit son dossier d'emploi. La commissaire adjointe conclut que le dossier du plaignant a été éliminé conformément au *Règlement de l'aviation canadien* et que la plainte est non fondée. Elle recommande toutefois à la compagnie de fixer une période maximale de conservation de ce type de dossiers ainsi que de consigner et d'archiver l'information se rapportant à la destruction des dossiers, à savoir qui a détruit les dossiers

L'équipe des demandes de renseignements répond aujourd'hui à des demandes moins nombreuses mais nécessitant des réponses plus étoffées. Un système téléphonique automatisé a été instauré afin de répondre aux questions les plus fréquentes du grand public, comme les questions sur le vol d'identité, le télémarketing et le numéro d'assurance sociale. Notre site Web, est de plus en plus un outil clé, renfermant un large éventail de renseignements fort utiles.

Statistiques sur les demandes de renseignements  
Du 1<sup>er</sup> janvier au 31 décembre 2005

Demandes relatives à la LPRPD reçues par l'Unité des demandes de renseignements	
Demandes téléphoniques	4 597
Demandes écrites (lettres et télécopies)	1 088
Nombre total de demandes de renseignements reçues	5 685

Demandes relatives à la LPRPD fermées par l'Unité des demandes de renseignements	
Demandes téléphoniques	4 623
Demandes écrites (lettres et télécopies)	1 587
Nombre total de demandes de renseignements fermées	6 210

Suivi des enquêtes effectuées aux termes de la LPRPD

Depuis 2004, la Direction des enquêtes et des demandes de renseignements effectue un suivi auprès des organisations visées par la LPRPD afin d'établir si celles-ci respectent leurs engagements pris en cours d'enquête et de voir l'évolution de la mise en œuvre des recommandations proposées dans les lettres de conclusions du Commissariat. Le Commissariat s'attend à ce que le suivi incite davantage les organisations à prendre les mesures nécessaires pour régler les problèmes identifiés dans le cadre d'enquêtes. Il s'agit aussi d'une façon de consigner l'information sur les moyens qu'ont pris les organisations pour s'acquitter de leurs responsabilités en vertu de la LPRPD.

Voici quelques exemples de mesures découlant de nos recommandations :

- Une personne se plaint que son ancien employeur a accédé à son compte et apporté des changements par l'entremise d'un programme de récompenses. Dans sa lettre de conclusions, la commissaire adjointe recommande à



Cette illustration des délais de traitement des plaintes est troublante. Conformément à l'article 13 de la *LPRPD*, la commissaire doit, pour chaque plainte, présenter un rapport à l'intérieur de l'année qui suit le dépôt de la plainte. Comme le tableau l'indique, il s'écoule en moyenne un peu moins de 11 mois entre la date du dépôt d'une plainte et la date de la conclusion d'enquête ou de la décision qui convient. Certes, nous respectons nos obligations légales, mais nous pourrions nous accommoder d'une marge de manœuvre plus grande. Aussi, si on les examine de plus près, les chiffres révèlent que dans certaines catégories, les délais ont été dépassés. En fait, selon le tableau qui présente les données par conclusion/décision, il faut compter en moyenne plus d'une année pour traiter les plaintes qui nécessitent une enquête complète, c'est-à-dire les plaintes fondées, non fondées et résolues. (Pour ce qui est de la catégorie « hors juridiction », le délai de traitement s'explique par la complexité des faits et des enjeux légaux qui doivent être examinés. Lorsqu'il est clair qu'une plainte ne relève pas de notre compétence, les agents chargés des demandes de renseignements ne la transmettent pas à l'étape suivante de traitement. Si une plainte présentant un enjeu juridictionnel se rend à l'étape de l'enquête, c'est parce qu'il y a incertitude sur la juridiction.) La période de temps nécessaire à la réalisation d'une enquête dépend de plusieurs facteurs, y compris les changements à nos procédures et les problèmes liés aux ressources. Peu importe les raisons, cette question nous préoccupe. Aussi, déployons-nous de nombreux efforts pour traiter les plaintes à l'intérieur des délais imposés par la Loi.

## Demandes de renseignements

Au Commissariat, l'Unité des demandes de renseignements répond aux demandes sur l'application de la *LPRPD* et de la *Loi sur la protection des renseignements personnels*. Chaque année, le grand public et les organisations adressent au Commissariat des milliers de demandes d'information sur la protection des renseignements personnels dans le secteur privé.

En 2005, le Commissariat a reçu 5 685 demandes de renseignements liées à la *LPRPD*, ce qui représente moins de la moitié du total des demandes reçues en 2004 (soit 12 132 demandes). Les demandes reçues en 2004 sont également moins nombreuses qu'en 2003. Comme nous l'avons fait remarquer l'année dernière, cette diminution peut être attribuable au fait que les organisations visées par la *LPRPD* comprennent désormais mieux la Loi. En effet, en 2003 et en 2004, de nombreuses organisations ont fait des démarches pour être mieux orientées relativement à la *LPRPD* et à sa pleine mise en œuvre le 1<sup>er</sup> janvier 2004.



## Délai de traitement des plaintes

Le tableau qui suit indique le nombre moyen de mois nécessaires à la réalisation complète d'une enquête, de la date de réception de la plainte jusqu'à la conclusion de l'enquête ou toute autre prise de décision. Le premier tableau présente les délais par type de conclusion ou de décision, et le second tableau, par type de plainte.

Délais de traitement des plaintes pour la période s'échelonnant du 1<sup>er</sup> janvier au 31 décembre 2005, par conclusion ou décision

Conclusion ou décision	Délai moyen en mois
Non fondée	13,79
Résolue	13,21
Fondée	12,44
Hors juridiction	12,27
Réglée	10,17
Abandonnée	7,67
Réglée rapidement	2,53
<b>Moyenne globale</b>	<b>10,94</b>

Délais de traitement des plaintes pour la période s'échelonnant du 1<sup>er</sup> janvier au 31 décembre 2005, par type de plainte

Type de plainte	Délai moyen en mois
Possibilité de porter plainte	16,0**
Collecte	11,8
Exactitude	11,5
Utilisation et communication	11,4
Transparence	11,3*
Frais	11,0*
Accès	10,9
Conservation	10,8*
Consentement	10,1
Responsabilité	10,0*
Correction/annotation	9,9
Mesures de sécurité	8,8
Respect des délais	6,6
<b>Moyenne globale</b>	<b>10,9</b>

\* Au délai de traitement de ces catégories correspondent quatre plaintes ou moins.  
 \*\* Au délai de traitement de cette catégorie correspond une seule plainte.

Cette approche semble donner de bons résultats et nous a amenés à créer une nouvelle catégorie, soit la catégorie « fondée et résolue ». (Cette nouvelle catégorie n'apparaît pas dans les tableaux de cette année puisqu'elle a été créée à la fin de 2005.) Cette nouvelle catégorie, qui ne résulte pas d'un simple exercice de formulation, permet de montrer que presque toutes les organisations ont accepté les recommandations de la commissaire et qu'elles les ont mises en œuvre en temps opportun. Pour une personne dont la vie privée a été atteinte de façon irréversible, il s'agit d'une approche qui apporte davantage que le confort de savoir qu'une enquête est en cours; grâce à cette approche, la plainte devient en effet un moteur de changement et de renouvellement.

Le tableau sur les plaintes fermées montre que nous continuons de favoriser le règlement des plaintes en cours d'enquête. Nous avions affirmé l'année dernière que cette façon de faire permettait de composer avec la charge de travail liée aux plaintes. Cette année, comme en 2004, ce sont les plaintes réglées en cours d'enquête qui ont été les plus nombreuses. Des 401 plaintes fermées en 2005, 157 (39 %) ont été réglées en cours d'enquête. Ce chiffre comprend 38 % de plaintes relatives à la collecte et 35 % de plaintes relatives à l'utilisation et à la communication. Nous poursuivons nos efforts dans cette voie, car il s'agit d'un aspect fondamental de la fonction d'ombudsman et d'une façon d'aider les organisations à changer leur mentalité et à régler les problèmes avec leurs clients et employés.

Au cours de l'année, nous avons fermé 401 plaintes. Il s'agit d'une amélioration par rapport aux deux années précédentes et d'un changement par rapport aux trois dernières années, au cours desquelles nous avons reçu plus de plaintes que nous en avons fermé. En 2005, nous avons fermé autant de plaintes que nous en avons reçue. (Une plainte reçue au cours d'une année civile donnée n'est pas nécessairement fermée la même année, ce qui explique qu'il peut nous arriver de fermer plus de plaintes que nous en recevons par année.)

Cette situation nous a permis de réduire notre arriéré de plaintes, mais comme n'importe quelle organisation chargée de traiter des plaintes publiques, nous devons continuellement nous efforcer de parvenir à un équilibre entre les ressources dont nous disposons et les plaintes qui nous sont adressées jour après jour. En 2006, de nouvelles ressources nous seront affectées, mais notre objectif premier consiste à trouver des moyens de simplifier les procédures et de faire preuve de plus d'efficacité et d'efficience.

l'aboutissement des enquêtes. Les plaintes sont alors classées dans les catégories des plaintes « réglées en cours d'enquête », « résolues » ou « réglées rapidement ».

Ces chiffres deviennent plus évocateurs dès lors que l'on examine les types de plaintes. La majorité des plaintes sont classées dans les trois catégories suivantes : utilisation et communication (149 plaintes, ou 37 % du total des plaintes), accès (81 plaintes, ou 20 %) et collecte (66 plaintes, ou 16 %). Parmi celles-ci, ce sont les plaintes concernant l'accès – plaintes formulées par les personnes qui se voient refuser l'accès à leurs renseignements personnels par une organisation – qui se résolvent le plus facilement. Une organisation qui refuse à une personne l'accès à ses renseignements personnels peut facilement corriger la situation en accédant à la demande de la personne ou en prouvant que des exceptions légitimes s'appliquent à la situation. Cette facilité de résolution se traduit par la proportion relativement élevée (64 %) de plaintes réglées en cours d'enquête ou résolues par l'organisation. Il n'en demeure pas moins que la grande quantité de plaintes relatives à l'accès peut être inquiétante; il faut peut-être en conclure que certaines organisations éprouvent encore de la difficulté à saisir pleinement les responsabilités qui leur incombent en vertu de la *LPRPD*. Le nombre de plaintes résolues a toutefois de quoi nous encourager.

Les plaintes relatives à l'utilisation, à la communication et à la collecte inappropriées sont plus troublantes car plus difficiles à résoudre. Lorsque les renseignements personnels d'une personne sont communiqués de façon inappropriée, il est impossible de faire marche arrière. Impossible également de faire marche arrière lorsqu'il y a collecte inappropriée de renseignements. La commissaire a déterminé que les organisations se conforment à leurs obligations en vertu de la *LPRPD* (plaintes non fondées) dans seulement 26 % des cas de plaintes sur la collecte de renseignements et dans 21 % des cas de plaintes sur l'utilisation et la communication de renseignements.

Par conséquent, nous avons intensifié nos efforts en 2005 afin de trouver de nouvelles solutions conformes à la *LPRPD*. Nous avons mis en place une nouvelle procédure conformément à laquelle la commissaire exerce davantage de pressions sur les organisations afin que celles-ci modifient leurs pratiques afin que le problème ne se reproduise pas, évitant ainsi que des torts irréparables soient causés à d'autres personnes. Si une enquête révèle que la *LPRPD* n'a pas été respectée, la commissaire, avant même de rendre ses conclusions aux termes d'une enquête, intervient rapidement et recommande à l'organisation concernée des mesures correctives. L'organisation doit, à la demande de la commissaire et dans un délai que cette dernière aura fixé, indiquer la façon dont elle entend mettre en œuvre les recommandations. Une fois la réponse de l'organisation obtenue, la commissaire communique ses conclusions.

Les résumés des conclusions d'enquêtes réalisées par le Commissariat en vertu de la *LPRPDE* peuvent être consultés dans le site Web du Commissariat, à l'adresse suivante : [www.privcom.gc.ca](http://www.privcom.gc.ca).

## Conclusions par type de plainte

Que nous révèlent les plaintes à propos du respect de la *LPRPDE* dont font preuve les organisations? La prudence est de mise; il ne convient pas d'accorder une importance absolue aux chiffres, puisqu'au terme de nos enquêtes, certaines plaintes auront été jugées non fondées. Il semble donc plus approprié d'examiner les conclusions d'enquête. Le tableau qui suit présente les résultats des enquêtes effectuées en 2005 pour chacune des catégories de plainte.

### Plaintes fermées entre le 1<sup>er</sup> janvier et le 31 décembre 2005

	Abandonnée	Réglée rapidement	Hors juridiction	Non fondée	Résolue	Réglée en cours d'enquête	Fondée	TOTAL
--	------------	-------------------	------------------	------------	---------	---------------------------	--------	-------

Utilisation et communication	21	6	7	31	9	52	23	149
Accès	11	1	0	10	20	32	7	81
Collecte	7	3	5	17	4	25	3	66
Mesures de sécurité	4	3	2	3	3	12	3	30
Consentement	4	0	1	6	1	9	1	22
Exactitude	0	1	0	2	1	13	0	17
Délais	0	1	0	1	2	4	3	11
Correction/annotation	0	0	0	5	2	3	0	10
Responsabilité	1	0	0	0	3	0	0	4
Conservation	1	0	0	0	1	2	0	4
Frais	0	0	0	1	1	1	0	3
Transparence	0	0	0	1	0	2	0	3
Possibilité de porter plainte	0	0	0	0	0	0	1	1
TOTAL	49	15	15	77	47	157	41	401

Il convient de noter que, des 401 plaintes déposées, seules 77 d'entre elles (19 %) ont été jugées non fondées. En d'autres mots, la commissaire a pu établir que les organisations respectent leurs obligations en vertu de la *LPRPDE* dans moins d'un cas sur cinq. Il est toutefois plus difficile de déterminer avec certitude le nombre de cas où les organisations ne se conforment pas à leurs obligations. Le nombre de plaintes classées dans la catégorie des plaintes fondées est relativement peu élevé, soit 41 plaintes ou 10 % du total des plaintes, ce qui s'explique par le fait que les problèmes relatifs à la protection des renseignements personnels sont souvent résolus avant



## Définitions des conclusions et d'autres dispositions

Le Commissariat a élaboré des définitions de conclusions et de décisions afin d'expliquer les résultats des enquêtes effectuées conformément à la *LPRPDE* :

- **Non fondée.** L'enquête n'a pas permis de déceler des éléments de preuves qui suffisent à conclure qu'une organisation a enfreint les droits du plaignant en vertu de la *LPRPDE*.

- **Fondée.** L'organisation n'a pas respecté une disposition de la *LPRPDE*.
- **Résolue.** L'enquête a corroboré les allégations, mais avant la fin de l'enquête, l'organisation a pris des mesures correctives pour remédier à la situation, à la satisfaction du Commissariat, ou s'est engagée à prendre ces mesures.
- **Fondée et résolue.** La commissaire est d'avis, au terme de son enquête, que les allégations semblent fondées sur des preuves, mais fait une recommandation à l'organisation concernée avant de rendre ses conclusions, et l'organisation prend ou s'engage à prendre les mesures correctives recommandées. Il s'agit d'une catégorie qui ne figure pas dans les statistiques étant donné qu'elle n'existe que depuis la fin de 2005. Elle sera intégrée aux tableaux de l'année prochaine.

- **Réglée en cours d'enquête.** Le Commissariat aide à négocier, en cours d'enquête, une solution qui convient à toutes les parties. Aucune conclusion n'est rendue.
- **Abandonnée.** Il s'agit d'une enquête qui est terminée avant que toutes les allégations ne soient pleinement examinées. Une affaire peut être abandonnée pour toutes sortes de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire ou il est impossible de lui demander de fournir des renseignements supplémentaires, lesquels sont essentiels pour en arriver à une conclusion.
- **Hors juridiction.** L'enquête a démontré que la *LPRPDE* ne s'applique pas à l'organisation ou à l'activité faisant l'objet de la plainte.

- **Réglée rapidement.** Situation dans laquelle l'affaire est réglée avant même qu'une enquête officielle ne soit entreprise. À titre d'exemple, si une personne dépose une plainte concernant un sujet qui a déjà fait l'objet d'une enquête par le Commissariat et qui a été jugé conforme à la *LPRPDE*, nous donnons les explications nécessaires à la personne plaignante. Cette conclusion s'applique également lorsqu'une organisation, mise au courant des allégations, règle immédiatement la question à la satisfaction du plaignant et du Commissariat.



conservé les renseignements assez longtemps pour permettre à la personne d'y avoir accès.

- **Mesures de sécurité.** Une organisation n'a pas protégé les renseignements personnels qu'elle détient par des mesures de sécurité appropriées.

- **Délais.** Une organisation a omis de fournir à une personne l'accès aux renseignements personnels qui la concernent dans les délais prévus par la Loi.

- **Utilisation et communication.** Les renseignements personnels sont utilisés ou communiqués à des fins autres que celles auxquelles ils avaient été recueillis, sans le consentement de la personne concernée, et l'utilisation ou la communication de renseignements personnels sans le consentement de la personne concernée ne font pas partie des exceptions prévues dans la Loi.

## Plaintes reçues entre le 1<sup>er</sup> janvier et le 31 décembre 2005

Type de plainte	Nombre	Pourcentage
Utilisation et communication	143	35,75
Accès	80	20,00
Collecte	68	17,00
Mesures de sécurité	34	8,50
Consentement	21	5,25
Délais	18	4,50
Responsabilité	10	2,50
Transparence	8	2,00
Exactitude	5	1,25
Correction/annotation	5	1,25
Frais	3	0,75
Conservation	3	0,75
Possibilité de porter plainte	1	0,25
Autres	1	0,25
<b>Total</b>	<b>400</b>	<b>100,00</b>

Cette année, les plaintes les plus fréquentes ont eu trait à l'utilisation inappropriée ou communication de renseignements personnels. Ces plaintes, ainsi que celles qui découlent d'un refus d'accès ou de la collecte inappropriée de renseignements personnels, représentent près de 73 % de toutes les plaintes reçues. Les chiffres de l'année dernière présentent un portrait similaire, alors que ces types de plaintes représentaient 79 % du total des plaintes.

## Définitions des types de plaintes déposées en vertu de la LPRPDE

Les plaintes adressées au Commissariat sont classées en fonction des principes et des dispositions législatives de la LPRPDE qui sont présumées enfreintes :

- **Accès.** Une personne s'est vu refuser l'accès aux renseignements personnels qu'une organisation détient à son sujet ou n'a pas reçu tous les renseignements, soit en raison de l'absence de certains documents ou renseignements ou parce que l'organisation a invoqué des exceptions afin de soustraire les renseignements.
- **Responsabilité.** Une organisation a failli à l'exercice de ses responsabilités à l'égard des renseignements personnels qu'elle possède ou qu'elle garde ou elle a omis de désigner une personne responsable de surveiller l'application de la Loi.
- **Exactitude.** Une organisation a omis de s'assurer que les renseignements personnels qu'elle utilise sont précis, complets et à jour.
- **Possibilité de porter plainte.** Une organisation a omis de mettre en place les procédures ou les politiques qui permettent à une personne de porter plainte en vertu de la Loi ou elle a enfreint ses propres procédures et politiques.
- **Collecte.** Une organisation a recueilli des renseignements personnels non nécessaires ou les a recueillis par des moyens injustes ou illégaux.
- **Consentement.** Une organisation a recueilli, utilisé ou communiqué des renseignements personnels sans le consentement de la personne concernée ou elle a fourni des biens et des services à la condition que la personne consente à la collecte, à l'utilisation ou à la communication déraisonnable de renseignements personnels.
- **Correction/annotation.** L'organisation n'a pas corrigé, à la demande d'une personne, les renseignements personnels qu'elle détient à son sujet ou, en cas de désaccord avec les corrections demandées, n'a pas annoté les renseignements afin d'indiquer la teneur du désaccord.
- **Frais.** Une organisation a exigé plus que des frais minimaux pour fournir à des personnes l'accès à leurs renseignements personnels.
- **Conservation.** Les renseignements personnels sont conservés plus longtemps qu'il n'est nécessaire aux fins qu'une organisation a déclarées au moment de la collecte des renseignements ou, s'ils ont été utilisés pour prendre une décision au sujet d'une personne, l'organisation n'a pas

Nous espérons que cette diminution est attribuable à une connaissance accrue qu'ont les organisations de leurs obligations en vertu de la *LPRDP*. Cette meilleure sensibilisation comporterait au moins deux avantages. D'une part, cela voudrait dire que les organisations auront davantage tendance à adopter des pratiques de gestion des renseignements personnels conformes à la *LPRDP*. D'autre part, en cas de problèmes, les responsables de la protection de la vie privée au sein des organisations, davantage au fait de la *LPRDP*, seront peut-être plus à même de résoudre les problèmes directement avec les personnes concernées.

Avec le temps, la *LPRDP* deviendra sans doute mieux connue et mieux comprise. En 2005, on remarque une diminution des plaintes surtout dans les secteurs qui sont visés par la *LPRDP* depuis la toute première phase de mise en œuvre de cette loi, en 2001. La *LPRDP* s'applique depuis 2001 aux institutions financières, aux télécommunications et aux transports interprovinciaux et internationaux. Les institutions financières, qui sont les organisations qui manipulent la plus grande quantité de renseignements personnels, sont une fois de plus celles qui font le plus souvent l'objet de plaintes, bien que le nombre de celles-ci ne représentent qu'un peu plus de la moitié (53 %) du nombre de plaintes de 2004. Le taux de diminution du nombre de plaintes est similaire dans le secteur des transports (58 % du total de 2004) et des télécommunications (44 %). Dans le secteur de la santé, qui n'est visé par la Loi que depuis 2002, la diminution a été très rapide; nous n'avons enregistré que 11 % du nombre de plaintes reçues en 2004 (mais en raison du nombre peu élevé de plaintes, ces statistiques ne sont peut-être pas de bons indicateurs des tendances).

Le nombre de plaintes concernant les secteurs visés depuis moins longtemps a également diminué, sauf pour ce qui est du secteur des services d'hébergement, pour lequel le nombre de plaintes est demeuré à peu près égal à celui de l'année précédente. Dans le secteur de la vente au détail, les plaintes représentent 54 % du total des plaintes de 2004, ce qui pourrait révéler que le secteur s'est rapidement conformé aux principes de la *LPRDP*. Ailleurs, la diminution a été moins marquée. Le nombre de plaintes visant des compagnies d'assurances représente 73 % du nombre de plaintes déposées dans ce secteur en 2004. Quant aux plaintes visant des professionnels, elles représentent 87 % des plaintes de l'année précédente (ici encore, les tendances observées sont peut-être biaisées en raison du nombre peu élevé de plaintes).

# PLAINTES

En 2005, la LPRPD a été appliquée, pour une deuxième année, à toutes les activités commerciales effectuées dans les provinces n'ayant pas adopté une loi essentiellement similaire. L'année 2005 a été marquée par une diminution importante du nombre de plaintes déposées en vertu de la LPRPD. Nous avons reçu 400 plaintes en 2005, comparativement à 723 pour l'année civile précédente.

Plaintes reçues entre le 1 <sup>er</sup> janvier et le 31 décembre 2005 - Répartition par secteur		
	Nombre	Pourcentage
Institutions financières	113	28,25
Assurances	60	15,00
Télécommunications	55	13,75
Ventes	44	11,00
Transports	39	9,75
Services d'hébergement	17	4,25
Professionnels	13	3,25
Santé	4	1,00
Services	2	0,50
Location	1	0,25
Autres	52	13,00
<b>Total</b>	<b>400</b>	<b>100,00</b>

Nous n'avons que des hypothèses pour expliquer la diminution du nombre de plaintes. En 2004, le nombre de plaintes avait augmenté par rapport aux années précédentes, une hausse largement attribuable à la pleine mise en œuvre de la Loi et au fait que celle-ci couvrirait désormais de nouvelles activités comme les assurances, la vente au détail, les services d'hébergement ainsi que des professions comme le droit. Les 400 plaintes reçues en 2005, qui ne représentent que 55 % des plaintes reçues en 2004, demeurent malgré tout considérablement plus nombreuses que les plaintes déposées en 2001, en 2002 ou en 2003.





En septembre 2004, le Commissariat a indiqué à Industrie Canada qu'à son avis, la *Loi sur la protection des renseignements sur la santé* est essentiellement similaire à la *LPRPDE*. En novembre 2005, le gouverneur en conseil a pris un décret (C.P. 2005-2224, 28 novembre 2005) afin d'exclure les dépositaires de renseignements personnels sur la santé de l'Ontario de l'application de la *LPRPDE*. Par conséquent, les dépositaires ne sont pas visés par la *LPRPDE* lorsqu'ils recueillent, utilisent et communiquent des renseignements personnels sur la santé. Le commissaire à l'information et à la protection de la vie privée de l'Ontario est par conséquent responsable de veiller à l'application de la *Loi sur la protection des renseignements sur la santé*, ce qui comprend la tenue d'enquêtes sur les pratiques de gestion de l'information des dépositaires de renseignements personnels sur la santé de la province.

Le Commissariat à la protection de la vie privée du Canada continuera d'assurer la surveillance de la collecte, de l'utilisation et de la communication des renseignements personnels sur la santé qui circulent au-delà des frontières provinciales dans le cadre d'activités commerciales. Le Commissariat surveillera les mêmes activités effectuées par des organisations autres que les dépositaires.

- comprendre les dix principes énoncés à l'Annexe 1 de la *LPRPDE*;
- prévoir un mécanisme indépendant et efficace de surveillance et de recours auquel se rattachent des pouvoirs d'enquête;
- restreindre la collecte, l'utilisation et la communication de renseignements personnels à des fins appropriées et légitimes.

## Lois provinciales et territoriales essentiellement similaires à la loi fédérale et adoptées à ce jour

Conformément à l'article 25(1) de la *LPRPDE*, le Commissariat est tenu de déposer annuellement devant le Parlement un rapport sur « la mesure dans laquelle les provinces ont édicté des lois essentiellement similaires » à la Loi.

En novembre 2003, le gouverneur en conseil a pris un décret (C.P. 2003-1842, 19 novembre 2003) établissant que la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec est essentiellement similaire à la loi fédérale. Cette loi, antérieure à la *LPRPDE*, est entrée en vigueur le 1<sup>er</sup> janvier 1994. En 2003, les provinces de la Colombie-Britannique et de l'Alberta ont adopté des lois applicables à toutes les organisations de ces deux provinces, à l'exception des organisations assujetties à d'autres lois provinciales et à l'exception des installations, des ouvrages, des entreprises ou des secteurs d'activité fédérale toujours visés par la *LPRPDE*. Les deux lois, qui portent le même titre, soit *Personal Information Protection Act*, sont entrées en vigueur le 1<sup>er</sup> janvier 2004.

Le gouverneur en conseil a pris deux autres décrets (C.P. 2004-1163, 12 octobre 2004, et C.P. 2004-1164, 12 octobre 2004) afin que toutes les organisations autres que les installations, ouvrages, entreprises ou secteurs d'activité fédérale ne soient pas visées par la *LPRPDE* en Alberta et en Colombie-Britannique.

En Ontario, la *Loi sur la protection des renseignements sur la santé* est entrée en vigueur le 1<sup>er</sup> novembre 2004. Cette loi régit la collecte, l'utilisation et la communication des renseignements personnels sur la santé détenus par les dépositaires en Ontario. Les dépositaires sont les personnes et les organismes énoncés dans la *Loi sur la protection des renseignements sur la santé* qui, conformément à leurs pouvoirs ou à leurs fonctions, ont la garde de renseignements personnels sur la santé ou exercent un contrôle sur ces renseignements.

## LOIS PROVINCIALES ESSENTIELLEMENT SIMILAIRES À LA LOI FÉDÉRALE

Conformément à l'alinéa 26(2)b) de la *LPRPDÉ*, le gouverneur en conseil peut, par décret, exclure une organisation, une catégorie d'organisations, une activité ou une catégorie d'activités de l'application de la *LPRPDÉ* en ce qui a trait à la collecte, à l'utilisation ou à la communication de renseignements personnels dans une province ayant adopté une loi essentiellement similaire à la *LPRPDÉ*.

Cette disposition a pour objectif de permettre aux provinces et aux territoires de réglementer les pratiques de gestion des renseignements personnels des organisations qui exploitent des activités à l'intérieur de leurs frontières ainsi que de promouvoir l'uniformisation des normes de protection de la vie privée dans l'ensemble du Canada et des différents secteurs.

Si le gouverneur en conseil signe un décret à cette fin, la *LPRPDÉ* ne s'applique alors plus à la collecte, à l'utilisation ou à la communication de renseignements personnels que font les organisations visées par la loi provinciale applicable. Les renseignements personnels qui circulent d'une frontière nationale ou provinciale à une autre sont quant à eux toujours visés par la *LPRPDÉ*. Celle-ci continue de s'appliquer aux activités, dans les provinces, des installations, ouvrages, entreprises ou secteurs d'activité fédérale visées par des lois fédérales, comme les banques, les compagnies aériennes et les sociétés de radiodiffusion et de télécommunication.

### Processus d'évaluation des lois provinciales et territoriales

Industrie Canada a annoncé que, pour être jugées essentiellement similaires à la loi fédérale, les lois provinciales et territoriales doivent :

Canada sont invités à faire une demande de subvention pour effectuer des recherches sur différents enjeux liés à la protection de la vie privée. Les organismes sélectionnés au terme d'un processus de sélection rigoureux obtiennent les fonds voulus pour réaliser les travaux proposés.

En 2005, les projets suivants ont été financés :

Clinique d'intérêt public et de politique	Ottawa, Ontario	Université Ryerson	Toronto, Ontario	Évaluer la conformité des organisations à la LRPD <sup>1</sup> et mener des études sur l'industrie en croissance du courtage de données	La protection de la vie privée en milieu de travail : Le point de vue de l'employeur	Faire ressortir divers intérêts, questions et préoccupations qui incitent les employeurs à adopter de nouvelles technologies de surveillance en milieu de travail	Examen préliminaire des enjeux relatifs à la protection de la vie privée en milieu de travail au Canada	Étudier les problématiques liées à la protection de la vie privée en milieu de travail relativement aux technologies nouvelles et actuelles	Évaluation de l'application de la LRPD <sup>1</sup>	Comparer l'efficacité de la LRPD <sup>1</sup> aux régimes similaires d'autres juridictions	Usages sociaux de l'ADN dans le processus de formulation des politiques et analyse de deux projets de loi sur l'identification par les empreintes génétiques	Examen des utilisations sociales des renseignements d'identification génétique au moyen d'une analyse comparative de deux projets de loi sur l'identification par les empreintes génétiques
	d'Internet du Canada											
British Columbia Civil Liberties Association	Vancouver, Colombie-Britannique	Université de la Colombie-Britannique	Vancouver, Colombie-Britannique									
Université d'Ottawa	Ottawa, Ontario											

Les projets devraient se terminer en 2006. Le site Web du Commissariat présentera alors des liens permettant d'accéder aux travaux publiés.

## RECHERCHES SUR LES NOUVEAUX ENJEUX RELATIFS À LA PROTECTION DE LA VIE PRIVÉE

Dans le cadre de son Programme des contributions, le Commissariat a accordé en 2005 des fonds de 148 850 \$ à cinq organisations pour que celles-ci effectuent des recherches sur de nouveaux enjeux relatifs à la protection de la vie privée. Ce programme est prévu dans notre budget annuel depuis l'an 2000, mais n'est opérationnel que depuis 2004. Les recherches qui ont ainsi été rendues possibles portent sur l'industrie florissante du courtage de données, l'utilisation d'échantillons d'ADN, la surveillance en milieu de travail ainsi que sur l'application de la *LPRPD* et la conformité à celle-ci.

Lancé en juin 2004, le Programme en est à sa deuxième année d'existence. Il vise à appuyer les travaux de recherche des organismes sans but lucratif, de même que les travaux de recherche des établissements d'enseignement et les associations industrielles et commerciales, ainsi que des organismes de défense des consommateurs, des associations bénévoles et des organisations de défense des droits. De façon globale, l'objectif visé est la constitution d'une capacité nationale de recherche au Canada sur la vaste gamme des enjeux ayant des répercussions sur la protection de la vie privée.

Le Commissariat a pour mandat d'assurer la tenue et la publication de travaux de recherche sur la protection des renseignements personnels. Le Programme des contributions a été établi dans le cadre du budget du Commissariat en vertu de son pouvoir de mettre en place des programmes et d'adopter des mesures législatives, conformément à la *LPRPD*.

Au cours des deux dernières années, 520 440 \$ ont été versés dans le cadre du Programme des contributions. Les organismes de recherche de l'ensemble du



une demande d'exclusion; 2) les télécommunications faites dans l'unique but de recueillir des renseignements dans le cadre d'un sondage auprès du public.

Le projet de loi C-37 a obtenu la sanction royale le 25 novembre 2005. Nous en sommes très heureux, mais nous croyons que les exemptions affaiblissent inutilement la portée de la Loi.

#### \* *Le projet de loi C-57 et les institutions financières*

Le 15 novembre 2005, nous avons comparu devant le Comité permanent des finances de la Chambre des communes afin de commenter le projet de loi C-57, la *Loi modifiant certaines lois relatives aux institutions financières*. Ce projet de loi est venu modifier le cadre de gouvernance des banques, des sociétés de portefeuille bancaires, des compagnies d'assurances, des sociétés d'assurance de portefeuille, des compagnies de fiducie et de prêt ainsi que des associations coopératives de crédit. Le projet de loi a permis de moderniser les lois qui régissent ces institutions afin de leur donner toute l'efficacité des normes adoptées en 2001 pour les sociétés par actions en vertu de la *Loi canadienne sur les sociétés par actions*. Le projet a également modernisé certaines normes de gouvernance spécifiques aux institutions financières.

Le projet de loi C-57 ne contient que quelques dispositions sur la collecte, l'utilisation et la communication de renseignements personnels. Certaines dispositions obligent les directeurs ou les cadres d'une banque et de toute autre institution financière à rendre compte de tout intérêt qu'ils retirent dans le cadre d'une transaction ou d'un contrat important avec la banque ou l'institution financière. D'autres dispositions permettent aux actionnaires d'avoir accès à cette information. De plus, le projet de loi C-57 autorise les actionnaires à accéder aux renseignements personnels d'autres actionnaires, à condition que ce ne soit qu'aux fins énoncées dans le projet de loi.

Lors de notre comparution devant le Comité, le projet de loi ne nous a pas semblé susciter de préoccupations importantes relativement à la protection de la vie privée ni menacer les renseignements personnels du consommateur. Nous avons même affirmé que l'importance accordée à la gouvernance d'entreprise pouvait contribuer à favoriser la protection de la vie privée, car cela inciterait les entreprises à être davantage sensibilisées aux risques liés à de mauvaises pratiques de gestion. Les entreprises seraient aussi encouragées à déployer beaucoup plus d'efforts pour assurer la sécurité.

Le projet de loi C-57 a obtenu la sanction royale le 25 novembre 2005.

Le Comité n'a pas pu déposer son rapport final en raison du déclenchement de la dernière élection fédérale. Nous nous réjouissons à l'idée de poursuivre nos travaux avec le Comité lors de la reprise des travaux parlementaires.

✱ *Le projet de loi C-37 et la liste d'exclusion nationale*

Le 8 juin 2005, nous avons comparu devant le Comité permanent de l'industrie, des ressources naturelles, des sciences et de la technologie de la Chambre des communes afin de faire part de nos observations sur le projet de loi C-37, *la Loi modifiant la Loi sur les télécommunications*. Conformément à ce projet de loi, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) est autorisé à établir une liste d'exclusion nationale, à imposer une pénalité importante aux entreprises de télémarketing qui omettent de suivre les règles et à confier la gestion de la liste d'exclusion à un tiers du secteur privé. Une fois la liste opérationnelle, les Canadiennes et les Canadiens qui souhaitent ne pas être sollicités par téléphone par des entreprises offrant des biens ou des services pourront demander que leur numéro de téléphone figure sur la liste d'exclusion unique et centralisée que les entreprises de télémarketing devront se procurer, respecter et mettre à jour régulièrement. Des systèmes similaires sont en place aux États-Unis et en Grande-Bretagne.

Lorsque nous avons comparu devant le Comité, nous avons fait savoir que nous étions en faveur de la liste d'exclusion. Nous avons toutefois suggéré au Comité de consulter la population canadienne avant d'adopter les exemptions proposées à la liste. Lors de sa comparution, le Commissariat bénéficiait du soutien de quelque 10 commissaires canadiens à la protection de la vie privée qui souhaitaient tous la tenue de consultations auprès de la population canadienne sur les exemptions qui visent, par exemple, les organismes de bienfaisance, les sondeurs ou les entreprises ayant déjà des liens avec leurs clients.

Le projet de loi qui a été revu et adopté par le Parlement présente plusieurs exemptions à la liste d'exclusion. Ainsi, sont exemptées les télécommunications non sollicitées effectuées par ou au nom d'un organisme de bienfaisance, par un parti politique officiel, par un candidat à l'investiture, par un candidat à la direction ou un candidat d'un parti politique ou encore par un regroupement de membres d'un parti politique. Le projet de loi autorise également : 1) les télécommunications faites au destinataire si celui-ci a une relation d'affaires en cours avec la personne qui effectue la télécommunication et s'il n'a pas fait, auprès de cette dernière,

Commissariat espère continuer d'entretenir une relation de travail productive avec les membres de ce comité au cours de la 39<sup>e</sup> législature. Les enjeux relatifs à la protection de la vie privée étant de plus en plus nombreux et complexes, il est essentiel que le Parlement se penche sur ces enjeux et qu'il réfléchisse aux inquiétudes de la population canadienne.

La très grande majorité de nos comparutions devant des comités parlementaires se rapportaient à des questions sur des politiques et des projets de loi liés à la Loi sur la protection des renseignements personnels, mais dans trois cas, nous avons abordé des sujets concernant la LPRPDE.

✱ *Étude du Sénat concernant le secteur des services financiers*

Le 16 février 2005, nous avons comparu devant le Comité sénatorial permanent des banques et du commerce afin de contribuer à l'étude des enjeux de consommation dans le secteur canadien des services financiers. Le Sénat avait chargé le Comité d'examiner les répercussions des initiatives et des lois fédérales visant à protéger les consommateurs du secteur financier. En outre, le Comité devait déterminer l'efficacité des organismes chargés de la protection du consommateur et de la supervision de ce secteur.

Comme les statistiques sur les plaintes présentées dans notre rapport annuel le démontrent, ce sont les institutions financières qui font le plus souvent l'objet de plaintes. Il en est ainsi depuis 2001, année qui marque la première étape de l'entrée en vigueur de la LPRPDE. Néanmoins, comme nous l'avons souligné devant le Comité, il ne faut pas nécessairement en conclure que les institutions financières ne se conforment pas à la LPRPDE. Nous croyons plutôt que cette situation est attribuable à la quantité et au caractère délicat des renseignements personnels que les banques et les autres institutions financières doivent recueillir, au rôle central que celles-ci jouent dans nos vies quotidiennes et peut-être aussi à la complexité de nos liens avec ces institutions.

La plupart du temps, des plaintes sont déposées parce que certains employés omettent de suivre les politiques et les procédures établies par leur entreprise. Dans ces cas, on ne peut conclure à des problèmes systémiques. Lorsque les plaintes sont fondées, les institutions financières acceptent de suivre nos recommandations dans la plupart des cas. Comme nous l'avons indiqué au Comité, le Commissariat entretient généralement des relations très positives avec les institutions financières.

en septembre 2005. Le Commissariat sera quant à lui l'hôte de la Conférence internationale de 2007 des commissaires à la protection des données et de la vie privée. Il nous tarde déjà d'accueillir plus de 60 commissaires à la protection des données et leurs employés, des membres de groupes de défense du droit à la vie privée, des représentants du secteur des affaires et bien d'autres intervenants du Canada et des quatre coins de la planète. Avec eux, nous travaillerons à trouver des façons pratiques de mettre en œuvre des mesures pour la protection des données applicables en tout lieu et à toute forme de conservation de renseignements personnels. En concentrant nos efforts sur des enjeux technologiques comme la biométrie, l'identification par radiofréquence (IRF), les normes pour l'authentification et la gestion de l'identité ainsi que les dispositifs de surveillance, nous accélérerons la mise en œuvre des mesures nécessaires à la protection de la vie privée, ce qui fera en sorte de réduire les coûts pour les entreprises.

## Le déroulement de l'année au Parlement

L'année 2005 a été marquée par de nombreux échanges entre le Commissariat et le Parlement. L'une des composantes fondamentales de notre travail consiste à comparaître devant des comités du Sénat et de la Chambre des communes pour communiquer nos avis éclairés sur les répercussions de projets de loi sur la protection de la vie privée ou sur toute autre question de politique intéressant le Parlement.

Cette année, le Commissariat a été appelé à comparaître 16 fois devant des comités parlementaires, ce qui représente un défi considérable pour l'organisme de petite taille que nous sommes. La commissaire à la protection de la vie privée étant une haute fonctionnaire du Parlement, ces comparutions demeurent indissociables de son travail.

L'un des comités importants pour le Commissariat est le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Grâce à ce comité mis sur pied à la fin de 2004, les Canadiennes et les Canadiens ont désormais un comité permanent qui veille à leurs intérêts en matière de protection de la vie privée à la Chambre des communes. En 2005, la commissaire à la protection de la vie privée du Canada et d'autres représentants du Commissariat ont comparu quatre fois devant ce comité. Les comparutions visaient notamment à nous interroger et à examiner notre budget des dépenses et nos rapports annuels. Les députés composant le Comité avaient également de nombreuses questions et préoccupations relatives aux principaux défis et possibilités qui attendent les Canadiennes et les Canadiens en matière de protection de la vie privée. Le



en vue d'harmoniser les solutions internationales et nous visons d'ailleurs la coopération parmi les commissaires à la protection des données. En 2004, nous avons soulevé de graves préoccupations relativement à la *USA PATRIOT Act* et à son incidence sur le traitement des renseignements personnels détenus par des organisations situées tant au Canada qu'à l'étranger. Nous avons en outre fait part de la vaste étude qu'a menée le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique sur cette question. Il importe que les gouvernements fédéral et provinciaux gardent l'œil ouvert et demeurent vigilants quant à l'impartition du traitement de renseignements personnels.

Nous devons tous faire preuve d'une plus grande efficacité à l'échelle internationale afin de trouver des solutions aux problèmes que pose l'impartition des services, de la même façon que nous l'avons fait en cherchant des solutions juridiques au problème du blanchiment des capitaux et du financement des activités terroristes à l'échelle mondiale. Nos organismes chargés de la protection des renseignements personnels n'ont pas les ressources nécessaires (ni l'autorité légitime) pour poursuivre les responsables d'infractions au-delà de nos frontières; aussi avons-nous intérêt à harmoniser les normes et les approches internationales. Puisque le Canada profite énormément de l'impartition, nous sommes en bonne position pour proposer des solutions valables autant pour les exportateurs que pour les sociétés des données et les personnes. Il nous semble aussi plus important que jamais d'échanger avec les organismes internationaux qui ont à cœur d'accroître la coopération internationale dans plusieurs sphères. La commissaire a été invitée par l'Organisation de coopération et de développement économiques (OCDE) à jouer un rôle important dans la coopération transfrontalière, et les travaux à cette fin ont commencé à l'automne 2005. Toujours à cette fin, la commissaire a jointe responsable de la *LRPDE* a participé cette année à des réunions en Corée et à Hong-Kong au sujet des directives sur la protection des renseignements personnels de la Coopération économique de la zone Asie-Pacifique. Dans le cadre de cet événement, le gouvernement du Canada a mis à profit son savoir-faire et a exercé une influence positive. Conséquemment, ces directives se rapprochent désormais du modèle canadien de protection des renseignements personnels. La commissaire adjointe a également participé à une réunion sur la question des documents de voyage dont l'OCDE et l'Organisation de l'aviation civile internationale ont été les hôtes en Grande-Bretagne.

La commissaire, l'avocate générale des Services juridiques et la directrice de Recherche et Politiques ont participé à la Conférence internationale des commissaires à la protection des données et de la vie privée qui a eu lieu en Suisse



*La Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes (LRPCFAT)* restreint considérablement la protection que doivent assurer la *LPRPDE* et la *Loi sur la protection des renseignements personnels*. En raison du caractère confidentiel des activités du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), les plaintes provenant des citoyens perdent de leur validité et les pouvoirs d'enquête de la commissaire à la protection de la vie privée n'ont plus la même portée. Le rôle du CANAFE consiste à travailler à la détection, à la prévention et à la dissuasion du recyclage des produits de la criminalité, du financement des activités terroristes et de toute menace à la sécurité du Canada. Puisque le CANAFE peut agir en toute confidentialité, les Canadiennes et les Canadiens ne seront plus en mesure de savoir si de l'information les concernant est recueillie ou s'ils font l'objet d'une enquête. De part et d'autre, on cherche à obtenir, à l'insu des personnes, toutes sortes de renseignements pour la surveillance financière. Le Commissariat doit ramener le débat aux problèmes que ces pouvoirs de surveillance du gouvernement posent à l'égard de la protection de la vie privée, des problèmes trop souvent ignorés à l'heure actuelle.

En mai 2005, un groupe de travail composé de multiples intervenants et mis sur pied par le ministre de l'Industrie a fait état d'un an sur le problème du multipostage abusif communément appelé « pourriel ». Le Commissariat a participé aux travaux de ce groupe; notre équipe s'est réjouie de constater que le ministre s'était fermement engagé à lutter rapidement contre un problème qui mine la confiance à l'égard d'Internet et qui rend les utilisateurs d'ordinateurs vulnérables aux fraudes, au vol d'identité et même à l'installation de logiciels malveillants ou de logiciels espions qui envahissent subrepticement leurs ordinateurs et corrompent les données que ceux-ci contiennent. À l'instar d'autres enjeux aussi importants, le Commissariat a reçu relativement peu de plaintes concernant l'utilisation d'adresses de courriel sans le consentement de la personne concernée. Nous sommes néanmoins d'avis que le problème s'avère beaucoup plus grave que le nombre restreint de plaintes ne pourrait le laisser croire. Nous espérons faire avancer ce dossier auprès du gouvernement en 2006.

La plupart des pourriels proviennent de l'extérieur du Canada. Il s'agit d'un problème de poids puisqu'il est très difficile d'effectuer des enquêtes et de poursuivre les responsables de pourriels. Des difficultés semblables se présentent pour de nombreuses autres fraudes Internet et même dans le cas d'entreprises légitimes étrangères qui recueillent et traitent des renseignements personnels. Nous l'avons constaté lors de l'examen d'un certain nombre de plaintes déposées cette année en vertu de la *LPRPDE*. Par conséquent, nous consacrons désormais plus d'efforts

- De transmettre les communications interceptées aux organismes chargés de l'application des lois ainsi qu'au SCRS;
- De faire le retrait d'une communication ou d'isoler une communication d'autres communications si l'interception de la première est autorisée;
- De se doter des moyens nécessaires pour l'interception simultanée, par les personnes autorisées de multiples organismes nationaux chargés de l'application des lois et de la sécurité nationale, des communications d'utilisateurs multiples. Par exemple, une entreprise de télécommunication aurait été tenue de se doter des moyens nécessaires pour permettre à plusieurs organismes d'intercepter de multiples communications en même temps. Le projet de loi proposait de fixer l'interception maximale à une communication pour chaque tranche de 5 000 abonnés.

Le projet de loi a été proposé à la fin de 2005 et, même s'il n'a pas été adopté, il constitue l'exemple par excellence de la volonté du gouvernement de donner aux entreprises du secteur privé le rôle d'agent de l'État. Certes, la surveillance électronique des communications – soit l'écoute téléphonique – ne date pas d'hier, mais à l'ère du commerce électronique et de la prestation de multiples services Internet, l'information qui peut être révélée est beaucoup plus vaste que celle provenant de l'écoute téléphonique. Le projet de loi C-74 a suscité de nombreuses préoccupations; si une nouvelle version du projet est présentée, il est à prévoir que le Commissariat et de nombreux groupes de défense des libertés civiles feront à nouveau connaître leurs inquiétudes.

Nous avons également suivi avec intérêt les consultations du ministère des Finances sur l'amélioration du régime canadien de lutte contre le blanchiment des capitaux et le financement des activités terroristes en vue de satisfaire aux engagements internationaux du Canada. Le Canada fait partie du Groupe d'Action Financière (GAFI), un organisme intergouvernemental dont le mandat est de mettre en place des initiatives de lutte contre le blanchiment des capitaux et le financement des activités terroristes et d'effectuer la surveillance de ces initiatives. Dans notre lettre au ministre des Finances, nous avons fait valoir que les pays se différencient sur plusieurs plans et que l'industrie financière canadienne est réglementée par des lois efficaces en matière de protection de la vie privée applicables aux institutions et aux documents financiers. Nous avons reconnu qu'il faut éviter que le Canada ne devienne une sorte de paradis pour les blanchisseurs d'argent, mais nous avons aussi établi que nous ne pouvons pas adopter chacune des mesures proposées par le GAFI sans d'abord nous interroger sur l'incidence qu'elles auraient sur la protection de la vie privée.

servent à transmettre et concernant la fourniture de renseignements sur les abonnés de services de télécommunication. Bien qu'il soit mort au feuilleton lorsque l'élection fédérale a été déclenchée en janvier 2006, le projet pourrait être présenté de nouveau, tel quel ou modifié.

Conformément à ce projet de loi, les fournisseurs de services de télécommunication auraient été tenus de mettre en place et de maintenir les moyens nécessaires à l'interception licite d'information transmise par la voie de télécommunications. En outre, ils auraient été tenus de communiquer des renseignements de base sur leurs abonnés à la Gendarmerie royale du Canada (GRC), au Service canadien du renseignement de sécurité (SCRS), au commissaire de la concurrence et à tout service de police constitué en vertu d'une loi provinciale. Avec ce projet de loi, les normes qui régissent l'accès aux renseignements personnels et leur communication et qui constituent actuellement une garantie de vie privée auraient été affaiblies. Les principales dispositions étaient les suivantes :

- Exiger de tous les fournisseurs de services de communication à fil, sans fil ou par Internet ainsi que de tous les autres fournisseurs de services de télécommunication de disposer des moyens nécessaires à l'interception d'information et d'adapter ces moyens lorsqu'ils modernisent leurs réseaux. Une vérification aurait été effectuée pour s'assurer de la conformité des fournisseurs à cette exigence;
- Donner aux organismes chargés de l'application des lois, c'est-à-dire la GRC et tout service de police constitué en vertu d'une loi provinciale, le SCRS ou le commissaire de la concurrence, les moyens d'exiger des fournisseurs de services de télécommunication, sans autorisation judiciaire, qu'ils fournissent certains renseignements de leurs abonnés (nom, numéro de téléphone, adresse, courriel, adresse IP) sur demande. Il s'agirait d'un changement par rapport à ce qui prévalait actuellement, car, conformément à l'alinéa 7(3)c.1) de la *LPRPDE*, les entreprises peuvent refuser toute demande d'accès en l'absence d'autorisation judiciaire. Le projet de loi C-74 prévoyait l'élimination de cette disposition.

L'ancien projet de loi C-74 aurait également exigé des fournisseurs de services de télécommunication :

- De se doter des moyens nécessaires pour l'interception des communications produites ou transmises par l'entremise de leur réseau;

Ces systèmes d'information traversent les frontières organisationnelles et juridictionnelles et redéfinissent les paramètres du temps et de l'espace. Il est maintenant possible de conserver des dossiers indéfiniment, d'y accéder par des nœuds délocalisés ainsi que de les combiner et de les rassembler afin de surveiller pratiquement tous les aspects de la vie privée. Des systèmes de forage de données et de tableur comparatif des renseignements personnels permettent de catégoriser, de trier et de classer les gens et d'en déduire et d'émettre des jugements prédictifs sur les attitudes et les comportements individuels. Bon nombre de ces systèmes font appel à la biométrie pour fouiller en profondeur la vie personnelle et l'identité.

La commissaire a également comparu devant le Sous-comité de la sécurité publique et nationale de la Chambre des communes le 5 juin 2005 pour commenter la Loi *antiterroriste* et émettre certaines réserves. Elle s'est notamment inquiétée de la surveillance exercée par les organismes investis de pouvoirs spéciaux en vertu de la Loi *antiterroriste*. Tout au long de l'année, le Commissariat a également exprimé ses préoccupations quant à l'érosion de la LPRPD induite par l'accès du gouvernement à des bases de données du secteur privé contenant des renseignements personnels. Nous nous inquiétons sérieusement de ce que des renseignements d'abord recueillis à des fins privées ou commerciales se retrouvent ensuite entre les mains du gouvernement. Si la frontière entre les secteurs public et privé s'estompé, des entreprises privées pourraient être amenées à jouer le rôle d'agents de l'État sans toutefois avoir à respecter les mesures de protection fondamentales d'une démocratie. Il faut contre cet accès du gouvernement aux données du secteur privé. On justifie le recours à des pouvoirs envahissants en invoquant des motifs en apparence convaincants, comme les attaques terroristes ou les pandémies imminentes, mais le besoin réel de tels pouvoirs est le plus souvent contestable.

D'aucuns affirmeront que la Loi sur la protection des renseignements personnels peut faire contrepois à ces pouvoirs envahissants. Mais cette loi, qui régit les activités gouvernementales de collecte et de gestion de renseignements personnels, a plus de 20 ans; elle est désuète et ne suffit plus à assurer la protection nécessaire et à réparer les torts causés. La Loi a été rédigée avant même l'apparition des ordinateurs de bureau et de toute la gamme des nouvelles solutions technologiques de surveillance qu'on active à l'aide d'une simple touche de clavier.

Le 15 novembre 2005, le ministre de la Sécurité publique et de la Protection civile du Canada a présenté le projet de loi C-74, Loi régissant les installations de télécommunication en vue de faciliter l'interception licite de l'information qu'elles



## À la défense de la vie privée

Cette année encore, les activités en matière de recherche et de politiques ont porté sur la disposition visant à accroître la capacité des organismes chargés de l'application des lois et de la sécurité nationale d'obtenir des renseignements personnels. Nous avons examiné de façon approfondie cette question dans le rapport annuel de 2004-2005 sur la Loi sur la protection des renseignements personnels; nous nous y pencherons de nouveau dans le prochain rapport annuel sur cette loi. Cette question requiert notre attention, car les lois présentées ou discutées au Parlement cette année tendent à contraindre les organisations du secteur privé à communiquer des renseignements personnels.

La commissaire a comparu devant le Comité spécial du Sénat sur la *Loi antiterroriste* le 9 mai 2005. L'énoncé de position du Commissariat met en lumière l'augmentation des pouvoirs en matière de surveillance électronique du gouvernement, lequel cherche à accéder aux banques de données personnelles du secteur privé :

Depuis les attentats du 11 septembre, le gouvernement canadien a instauré une série de mesures pour renforcer son pouvoir de surveillance des citoyennes et des citoyens, de même que des résidentes et des résidents du Canada. Il a également investi considérablement dans le développement de systèmes intégrés d'information qui collectent, traitent et échangent les renseignements personnels des citoyennes et des citoyens, de même que des résidentes et des résidents : résidents, portant sur des aspects variés de leur vie économique et civique : déplacements, investissements, consommation, prestations de programmes sociaux, pour ne nommer que ceux-là.





## Analyse de rentabilisation : ressources

Au terme d'une analyse exhaustive, qui comprenait l'examen du processus opérationnel lié aux fonctions d'enquêtes et de demandes de renseignements ainsi que l'examen approfondi de toutes les autres fonctions, le Commissariat a demandé une augmentation de plus de 50 % de ses ressources. Le Commissariat prévoit actuellement ses activités en fonction d'une augmentation de ses ressources d'ici les deux prochaines années, souhaitant pouvoir compter sur une équipe composée d'environ 140 employés et sur un budget annuel global d'environ 18 millions de dollars.

Il est impératif que le Commissariat obtienne des fonds accrus, stables et à long terme, non seulement pour l'organisme lui-même, mais aussi pour les Canadiennes et les Canadiens ainsi que pour les organisations visées par les lois fédérales sur la protection de la vie privée. En effet, le Commissariat entend se défaire de son approche réactive et fondée sur les plaintes, au profit d'une approche proactive et multidisciplinaire correspondant davantage au mandat que lui a confié le Parlement.

Le Commissariat a procédé à deux importantes analyses : le document Vision et plan de service institutionnel ainsi que l'analyse de rentabilisation en vue d'un financement permanent. Ces deux documents définissent notre rôle tel qu'il doit être, en tant que représentant du Parlement au service des intérêts des Canadiennes et des Canadiens, et ce dont nous avons besoin pour atteindre nos objectifs.

Doté de fonds adéquats, le Commissariat pourra effectuer les activités suivantes, conformément à la LPRPD :

- mener un nombre significatif de vérifications et d'examins pour promouvoir une plus grande conformité et contribuer à l'élaboration d'un solide cadre de gestion de la protection de la vie privée dans le secteur privé;
- effectuer des analyses de nature juridique et politique de lois et de projets de loi afin d'appuyer les travaux du Parlement;
- avoir recours, de façon plus proactive, efficace et importante, aux outils d'application de la loi que lui a confiés le Parlement, comme les plaintes émanant de la commissaire, les poursuites en justice et la communication d'information d'intérêt public;
- effectuer des recherches sur les nouvelles tendances et les nouveaux enjeux relatifs à la protection de la vie privée afin d'aider les citoyens et les décideurs à mieux comprendre les défis d'aujourd'hui et de demain dans cette sphère;
- contribuer à de vastes projets de sensibilisation du grand public visant à mieux informer les personnes de leurs droits et à mieux informer les organisations de leurs obligations;
- utiliser un processus d'enquête simplifié pour s'attaquer à l'arrière des plaintes;
- soutenir les efforts de renouvellement organisationnel.

## Vision du Commissariat à la protection de la vie privée du Canada

Nous travaillons à embaucher de nouveaux talents et à nous adjoindre des personnes hautement qualifiées. Nous avons mené à terme un ambitieux programme qui visait à corriger toutes les lacunes au sein de la direction de l'organisme. Jusqu'ici, les vérifications et les évaluations du Commissariat effectuées par le Bureau du vérificateur général du Canada, la Commission de la fonction publique ainsi que par la Commission canadienne des droits de la personne ont été positives. Nous avons aussi mis en œuvre un processus réfléchi et systématique pour déterminer nos besoins organisationnels. Le Commissariat est à nouveau une institution digne de la confiance du Parlement et de la population canadienne dont il sert les intérêts.

## NOTRE MANDAT RENFORCÉ

Jusqu'ici, le Commissariat n'a pas obtenu les fonds permanents nécessaires pour s'acquitter des responsabilités que lui confère la *LPRPD*. Des fonds ne lui ont été accordés que pour trois ans. La *LPRPD*, dont l'application s'est échelonnée en plusieurs étapes, est entrée en vigueur en 2001 et a atteint sa pleine mise en œuvre en 2004. Il nous semblait important de laisser retomber la poussière avant de définir nos besoins financiers à long terme. La *LPRPD* est pleinement en vigueur depuis maintenant deux ans, et les demandes qui nous sont adressées en vertu de cette loi sont de plus en plus nombreuses. Notre capacité financière actuelle ne nous permet pas de répondre aux exigences d'un mandat aux multiples facettes. Conséquemment, nous devons composer avec un arriéré considérable de plaintes à traiter; les personnes qui ont déposé ces plaintes commencent à s'impatisser, ce que nous comprenons sans peine. L'équipe des vérificateurs est trop réduite pour nous permettre d'effectuer des vérifications efficaces en vue d'assurer la conformité. Bien que nous ayons mis en place une approche axée sur la gestion du risque, il nous faut intensifier nos activités de vérification. De plus, en raison des restrictions financières, notre stratégie de communication est essentiellement réactive, alors que c'est d'une stratégie proactive de sensibilisation du grand public sur les droits et les obligations en matière de protection de la vie privée dont nous avons besoin. Pour leur part, la Direction de la recherche et des politiques ainsi que la Direction des services juridiques, plutôt que de composer efficacement avec tout nouveau problème relatif à la protection de la vie privée, se limitent à répondre aux urgences.

Les dernières années ont été éprouvantes pour le Commissariat. Mais à quelque chose malheur est bon : les difficultés nous ont permis de revoir de fond en comble les façons de faire du Commissariat. Celui-ci en ressort renouvelé et engagé sur la bonne voie. Il est maintenant temps d'instaurer la nouvelle vision du Commissariat, ce qui nécessitera toute une gamme d'outils afin de la mettre en œuvre.

les évaluations des renseignements personnels, la communication d'information publique et la sensibilisation du grand public afin d'aider celui-ci à exercer un certain contrôle sur ses renseignements personnels et les entreprises à respecter leurs obligations. Nous effectuons aussi des travaux de recherche sur les nouveaux enjeux et, au besoin, nous prenons des mesures juridiques.

Le mandat qui nous est confié en vertu de la *LPRPD* est vaste et exigeant, et notre incertitude financière ne nous a pas permis d'aller aussi loin que nous l'aurions souhaité. La réalisation des activités en vertu de la *LPRPD* n'a pas été appuyée par un financement permanent, et ce n'est qu'en 2003 que des fonds à cette fin ont été affectés puis renouvelés chaque année. La Loi est pleinement en vigueur depuis 2004, et les demandes sont de plus en plus nombreuses. Nous avons donc sollicité une augmentation pluriannuelle importante de notre base de financement, et nous prévoyons une croissance importante. Un financement adéquat nous permettra de respecter le mandat que nous accorde la Loi et de réagir aux pressions du gouvernement et des groupes commerciaux toujours plus avides de renseignements personnels.

Je souhaite remercier l'honorable Gérard V. La Forest pour son excellente étude sur la possibilité de fusion du Commissariat à l'information du Canada et du Commissariat à la protection de la vie privée du Canada. Il a conclu que la structure qui convient le mieux pour faire appliquer les lois canadiennes en matière de protection des renseignements personnels demeure celle conçue précisément pour la protection de la vie privée. Le fait de conserver cette structure permet aussi d'éviter les bouleversements administratifs qui auraient résulté de la fusion des deux entités. Pour l'heure, il est beaucoup plus important que le Commissariat se concentre sur les préoccupations actuelles touchant le domaine de la vie privée et qu'il se prépare à traiter les nombreux autres enjeux qui ne manqueront pas de surgir.



contrôle efficace sur les transactions qui, par la voie de l'Internet, passent outre les frontières du pays, entraînent la manipulation de renseignements personnels de la population canadienne et échappent à la portée de la *LPRPD*.

Le Commissariat à la protection de la vie privée du Canada (le Commissariat) poursuit son travail en faveur de la protection de la vie privée grâce à l'éducation, à la sensibilisation, à la résolution de plaintes et à l'adoption de mesures préventives. À titre d'ombudsman, j'encourage la conformité volontaire aux principes de protection des renseignements personnels ainsi que l'adaptation de ces principes aux besoins particuliers de l'industrie et des consommateurs. Je suis très heureuse de constater que la propension à résoudre les plaintes adressées au Commissariat semble vouloir se poursuivre. Près de la moitié de l'ensemble des plaintes sont en effet résolues à la satisfaction de toutes les parties concernées.

Les normes de protection de la vie privée sont de mieux en mieux connues, et l'on s'attend de plus en plus à ce qu'elles soient respectées. Il est désormais inacceptable d'omettre de prendre des mesures correctives directes lorsque la protection des renseignements personnels est négligée. En 2005, j'ai décidé de demander aux organisations visées par des plaintes fondées d'énoncer les mesures qu'elles songeaient à prendre, avec l'intention de porter la plainte devant la Cour fédérale au besoin. À ce jour, dans les quelques situations où j'ai dû adopter cette approche, presque toutes les organisations se sont rapidement engagées à prendre les mesures nécessaires et à revoir en profondeur leur façon de fonctionner.

Egalement, nous vérifions de façon continue si les changements recommandés par suite de plaintes d'années précédentes ont bien été mis en œuvre. Ici encore, le niveau de conformité est élevé et, lorsque nous intervenons par suite d'une plainte, la coopération des organisations concernées est généralement fort louable.

Il reste néanmoins difficile, voire impossible, pour la population de se plaindre de l'utilisation de ses renseignements personnels si elle ne saisit pas bien la façon dont les renseignements sont utilisés. Dans notre monde hautement technologique et opaque, seuls quelques experts sont véritablement en mesure de comprendre les tenants et les aboutissants de la circulation et de l'utilisation des renseignements personnels. Puisque les Canadiennes et les Canadiens ne comprennent pas pleinement tous les aspects du traitement de leurs renseignements personnels, le Commissariat doit se rapporter à des indicateurs de problèmes autres que les plaintes provenant du public. Par conséquent, nous avons recours à différents outils, comme les vérifications, l'examen des systèmes de gestion de l'information,

En 2006, le Parlement procédera à l'examen de la *LPRPDE*. Cet examen revêt un caractère essentiel, car nous aurons la chance unique de vérifier si la Loi permet d'assurer aux Canadiennes et aux Canadiens que leur droit à la protection de la vie privée, qui leur est si cher, est bien protégé. En outre, les parlementaires et la population pourront examiner les solutions possibles aux atteintes de plus en plus nombreuses qui visent les renseignements personnels et la vie privée de tous et chacun, soit le vol d'identité, les pourriels et les activités électroniques frauduleuses.

Même s'il ne s'agit pas d'une panacée, la *LPRPDE* et les lois provinciales qui lui sont essentiellement similaires ont permis de changer en profondeur les comportements et les perceptions concernant la protection des renseignements personnels au Canada. En effet, les Canadiennes et les Canadiens s'attendent désormais à ce que les organisations qui utilisent leurs renseignements personnels expliquent et justifient leurs actions. Ils s'expriment également beaucoup plus qu'auparavant sur la question et savent davantage de quoi il retourne.

Les dernières années ont été synonymes de défis pour les organisations visées par la *LPRPDE* qui ont travaillé, à leur propre rythme et en obtenant divers degrés de succès, à mettre en œuvre les principes de la Loi. Dans l'ensemble, les organisations canadiennes se conforment dans une très large mesure aux obligations qui leur sont imposées en vertu de la *LPRPDE*. Les entrepriises, de petite et de grande taille, ont fait preuve de bonne volonté et d'engagement en faveur des valeurs collectives; elles ont aussi démontré qu'elles étaient ouvertes aux changements nécessaires à la protection de la vie privée. Je crains toutefois que la conformité apparente ne soit pas nécessairement garante de pratiques véritablement efficaces en matière de sécurité et de protection de la vie privée. La bonne volonté doit maintenant se traduire par des actions concrètes.

En raison des nouvelles technologies, des tendances de consommation et des inquiétudes relatives à la sécurité nationale, on ne cesse de trouver de nouveaux motifs de recueillir et d'utiliser un nombre toujours plus grand de renseignements personnels. Il nous faut donc revoir nos définitions et l'application de nos règles de fonctionnement. Dans quelle mesure ces règles sont-elles appropriées à l'ère de l'Internet, des mini-ordinateurs de voiture, des dispositifs de localisation cousus aux vêtements, de la surveillance de voisinage par satellite et de l'impartition du traitement de renseignements dans des pays où la protection de ceux-ci n'est pas assurée? Même si le Canada se dote d'un cadre efficace de protection des renseignements personnels, il n'est pas nécessairement en mesure d'étendre sa protection au-delà de ses frontières. En outre, il ne peut pas non plus exercer un

J'aimerais pouvoir dire que dans le domaine de la protection de la vie privée au Canada, tout va pour le mieux dans le meilleur des mondes possible. Malheureusement, ce n'est pas encore le cas. Plus que jamais, les Canadiennes et les Canadiens s'inquiètent du sort de leur vie privée et du risque que leurs renseignements personnels soient utilisés à mauvais escient. Leurs inquiétudes sont le fruit de menaces toujours plus nombreuses surgissant à l'ère électronique de la circulation massive et continue de données.



La loi actuelle adoptée pour protéger les renseignements personnels dans le secteur privé n'offre qu'une partie de la solution. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) est pleinement en vigueur depuis maintenant deux ans et protège les différents aspects de la vie privée de l'ensemble de la population canadienne, sauf au Québec (qui a adopté sa propre loi pour la protection des renseignements personnels dans le secteur privé en 1994). En vertu de la Loi, les organisations doivent désormais se conformer à une série d'obligations applicables à la collecte, à l'utilisation et à la communication de renseignements personnels.

Dans la foulée de la LPRPDE, plusieurs provinces ont voulu adopter leur propre loi, des lois subséquemment jugées « essentiellement similaires » à la LPRPDE. Ainsi, la Colombie-Britannique et l'Alberta ont l'une et l'autre adopté une loi en 2003, puis ce fut le tour de l'Ontario en 2005 (pour la protection des renseignements personnels sur la santé).

41	Vérification et revue .....
42	L'utilisation de dispositifs d'identification par radiofréquence au Canada .....
43	L'identification par radiofréquence au Canada .....
45	Nécessité de faire connaître l'IRF et d'en définir l'orientation .....
45	Vérification de suivi de la Banque Canadienne Impériale de Commerce .....
46	Gestion des renseignements personnels : autoévaluation .....
47	Devant les tribunaux.....
47	Demandes en vertu de la LPRPD.....
47	Dossiers en cours.....
48	Nouveaux dossiers d'intérêt .....
52	Demandes abandonnées.....
54	Révisions judiciaires .....
57	Communications et sensibilisation du grand public.....
58	Recherche sur l'opinion publique .....
58	Discours et événements spéciaux .....
59	Publications .....
60	Site Web .....
61	Gestion intégrée .....
61	Planification et présentation de rapports .....
61	Ressources humaines .....
62	Finances et administration.....
63	Gestion de l'information et technologie de l'information (GI/TI) .....
63	Besoins en ressources .....
63	Information financière .....

TABLE DES MATIÈRES

Avant-propos..... 1

Notre mandat renforcé..... 5

Politiques ..... 9

    À la défense de la vie privée ..... 9

    Le déroulement de l'année au Parlement ..... 15

Recherches sur les nouveaux enjeux relatifs à la protection de la vie privée..... 19

Lois provinciales essentiellement similaires à la loi fédérale ..... 21

    Processus d'évaluation des lois provinciales et territoriales ..... 21

    Lois provinciales et territoriales essentiellement similaires ..... 22

        à la loi fédérale et adoptées à ce jour..... 22

Plaintes..... 25

    Définitions des types de plaintes déposées en vertu de la LPRPDE ..... 27

    Définitions des conclusions et d'autres dispositions..... 29

    Conclusions par type de plainte..... 30

    Délai de traitement des plaintes ..... 33

    Demandes de renseignements ..... 34

    Suivi des enquêtes effectuées aux termes de la LPRPDE ..... 35

    Processus d'enquête en vertu de la LPRPDE ..... 38







Mai 2006

L'honorable Peter Milliken, député  
Président  
Chambre des communes  
Ottawa  
Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel sur la Loi sur la  
*protection des renseignements personnels et les documents électroniques* du Commissariat à  
la protection de la vie privée du Canada pour la période s'échelonnant du 1<sup>er</sup> janvier au  
31 décembre 2005.

Veillez agréer, Monsieur, l'assurance de ma considération distinguée.

*Jennifer Stodart*  
Jennifer Stodart  
Commissaire à la protection  
de la vie privée du Canada





Mai 2006

L'honorable Noël A. Kinsella, sénateur  
Président  
Sénat du Canada  
Ottawa  
Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel sur la Loi sur la  
*protection des renseignements personnels et les documents électroniques* du Commissariat à  
la protection de la vie privée du Canada pour la période s'échelonnant du 1<sup>er</sup> janvier au  
31 décembre 2005.

Veuillez agréer, Monsieur, l'assurance de ma considération distinguée.

Jennifer Stoddart

Jennifer Stoddart  
Commissaire à la protection  
de la vie privée du Canada

Commissariat à la protection de la vie privée du Canada  
112, rue Kent  
Ottawa (Ontario)  
K1A 1H3

(613) 995-8210, 1 800 282-1376  
N° de téléc. : (613) 947-6850  
ATS : (613) 992-9190

© Ministère des Travaux publics et Services gouvernementaux Canada 2006  
N° de cat. : IP51-1/2005-1  
ISBN : 0-662-69647-6

Ce document peut être consulté dans notre site Web, à l'adresse suivante :  
[www.privcom.gc.ca](http://www.privcom.gc.ca).



Commissaire à la protection  
de la vie privée du Canada



Privacy Commissioner  
of Canada

# Rapport annuel au Parlement 2005



Rapport sur la  
loi sur la protection des  
renseignements personnels  
et les documents électroniques

Canada



RAPPORT SUR LA  
Loi sur la protection des  
renseignements personnels  
et les documents électroniques



# Rapport annuel au Parlement 2005

Vie Privée



Privacy Commissioner  
of Canada



Commissaire à la protection  
de la vie privée du Canada

CA1  
PC  
A574

# Privacy

ANNUAL REPORT TO PARLIAMENT

2007

Report on the  
*Personal Information  
Protection and  
Electronic Documents Act*







Privacy Commissioner  
of Canada



Commissaire à la protection  
de la vie privée du Canada

# Privacy

ANNUAL REPORT TO PARLIAMENT

2007

Report on the  
*Personal Information  
Protection and  
Electronic Documents Act*



Office of the Privacy Commissioner of Canada  
112 Kent Street  
Ottawa, Ontario  
K1A 1H3

(613) 995-8210, 1-800-282-1376  
Fax (613) 947-6850  
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2008  
Cat. No. IP51-1/2007  
ISBN 978-0-662-05757-4

This publication is also available on our website at [www.privcom.gc.ca](http://www.privcom.gc.ca).

**Privacy Commissioner  
of Canada**

112 Kent Street  
Ottawa, Ontario  
K1A 1H3  
Tél.: (613) 995-8210  
Fax: (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca

**Commissaire à la protection  
de la vie privée du Canada**

112, rue Kent  
Ottawa (Ontario)  
K1A 1H3  
Tél. : (613) 995-8210  
Télééc. : (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca



June 2008

The Honourable Noël A. Kinsella, Senator  
The Speaker  
The Senate of Canada  
Ottawa



Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2007.

Yours sincerely,

*Jennifer Stoddart*

Jennifer Stoddart  
Privacy Commissioner of Canada



**Privacy Commissioner  
of Canada**

112 Kent Street  
Ottawa, Ontario  
K1A 1H3  
Tél.: (613) 995-8210  
Fax: (613) 947-6850  
1-800-282-1376  
[www.privcom.gc.ca](http://www.privcom.gc.ca)

**Commissaire à la protection  
de la vie privée du Canada**

112, rue Kent  
Ottawa (Ontario)  
K1A 1H3  
Tél. : (613) 995-8210  
Téléc. : (613) 947-6850  
1-800-282-1376  
[www.privcom.gc.ca](http://www.privcom.gc.ca)



June 2008

The Honourable Peter Milliken, M.P.  
The Speaker  
The House of Commons  
Ottawa

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2007.

Yours sincerely,

A handwritten signature in cursive script that reads "Jennifer Stoddart".

Jennifer Stoddart  
Privacy Commissioner of Canada





# TABLE OF CONTENTS

---

Message from the Commissioner.....1

Privacy by the Numbers in 2007.....7

New Strategic Priorities.....9

Key Accomplishments in 2007 ..... 13

Key Issue: Data Breaches..... 17

    A Data Breach Investigation: The TJX Case.....21

    How our Office Helps Organizations Prevent Data Breaches..... 23

Improving *PIPEDA*..... 25

Complaint Investigations and Inquiries..... 29

Audit and Review ..... 43

In the Courts ..... 47

Substantially Similar Provincial and Territorial Legislation ..... 57

The Year Ahead..... 59

Appendix 1 – Definitions; Investigation Process ..... 61

    Definitions of Complaint Types under *PIPEDA* ..... 61

    Definitions of Findings and Other Dispositions ..... 62

    Investigation Process under *PIPEDA* ..... 64

Appendix 2 – Inquiry and Investigation Statistics ..... 67

*PIPEDA* Inquiries Received ..... 67

*PIPEDA* Inquiries Closed ..... 67

    Complaints Received by Type..... 68

    Complaints Received – Breakdown by Sector..... 69

    Closed Complaints by Type ..... 70

    Closed Complaints by Finding ..... 71

*PIPEDA* Investigation Treatment Times - By Finding ..... 72

    Findings by Complaint Type ..... 73

    Findings by Industry Sector..... 74

*PIPEDA* Investigation Treatment Times - By Complaint Type ..... 75



## MESSAGE FROM THE COMMISSIONER

The year 2007 will no doubt be remembered in the privacy world as the year of the data breach.

The size of some of the data spills reported around the globe was staggering: An estimated *94 million* credit and debit cards were exposed when hackers broke into the system at TJX Companies Inc., the U.S. retail giant which owns Winners and HomeSense stores in Canada. In the United Kingdom, two computer discs holding the personal details of some *25 million* child benefit recipients vanished.



Those were only the two most high-profile data security disasters. Scores of other major data breaches affecting millions of people around the world were also reported.

Data breaches here in Canada kept our team extraordinarily busy in 2007.

Of particular note, we investigated the TJX/Winners breach, as well as the disappearance of a hard drive containing the personal information of close to half a million clients of Talvest Mutual Funds, a subsidiary of the Canadian Imperial Bank of Commerce (CIBC).

### **An Obligation for Business**

It's clear that organizations of all sizes can – and must – do more to prevent data leaks.

The *Personal Information Protection and Electronic Documents Act (PIPEDA)* imposes a legal obligation on businesses to adequately safeguard the personal data they collect. Too often, however, we see breaches occur as a result of human error or a cavalier approach to security.

Our Office has been working with the business community in Canada to improve privacy practices and encourage the use of strong information technology safeguards.

Recent headlines about massive data breaches are also prompting some businesses to rethink how they handle privacy and security. No one wants to have to call clients to tell them that their personal information has been lost.

I hope 2008 will mark a turning point in the protection of personal information. It is time for businesses to recognize that personal information is valuable – and it needs to be well protected.

Unfortunately, the challenge of safeguarding personal information is greater than ever. The amount of personal data being collected, stored and shared is ever-growing – and so too is the ingenuity of fraudsters and hackers.

## **A Busy Year**

Our Office will also remember 2007 as the year we:

- Hosted the 29<sup>th</sup> International Conference of Data Protection and Privacy Commissioners;
- Expanded our work in the international arena;
- Contributed to efforts to improve *PIPEDA*; and
- Welcomed a new Assistant Privacy Commissioner.

A few thoughts on each of these key events and issues of the year...

## **Hosting the Privacy World**

The success of the 29<sup>th</sup> International Conference of Data Protection and Privacy Commissioners – held in Montreal in September and following through on our initial 2002 engagement – was beyond our highest expectations.

We welcomed more than 600 commissioners, academics, privacy professionals, advocates, government officials, IT specialists and others from around the globe – making it the largest-ever conference of its kind. Most importantly, the positive reviews and kudos from participants justified the time and resources invested in this event.

The conference theme was Privacy Horizons: *Terra Incognita*. Early cartographers marked unknown lands that had yet to be mapped with this Latin term. One of the earliest known terrestrial globes from Europe labels an uncharted edge of the ocean “*hic sunt dracones*” – or “here be dragons.”



This notion of an unknown landscape with lurking dragons seemed the perfect metaphor for the future of privacy.

Privacy issues are changing rapidly, with powerful new technologies and the international war on terror acting as potent forces which threaten the privacy of people around the world.

The goal of our conference was to begin to chart what the privacy world of the future might look like and also to equip privacy advocates with some strong dragon-slaying tools.

During a series of plenaries, workshops and information sessions, we considered the best strategies for defending privacy rights in the face of constant change.

Participants heard from the who's who of the privacy world, including security technology guru and author Bruce Schneier; Simon Davies, a pioneer of the international privacy arena and founder of Privacy International; consumer privacy advocate Katherine Albrecht; Marc Rotenberg, executive director of the Electronic Privacy Information Center; Peter Fleischer, Google's global privacy counsel; Peter Hustinx, the European Data Protection Supervisor; as well as Peter Schaar, now past-chair of the EU Article 29 Data Protection Working Party and France's Alex Türk, who is now chair of the working party.

Our guest of honour, on hand to help open the conference, was the Honourable Peter Milliken, Speaker of the House of Commons.

Our keynote speaker was U.S. Homeland Security Secretary Michael Chertoff, who bluntly argued his thoughts on balancing privacy rights in the context of national security to a somewhat skeptical audience – and sparked plenty of discussion throughout the conference!

A member of our external advisory committee, University of Ottawa law Professor Michael Geist, who holds the Canada Research Chair of Internet and E-commerce Law, later responded by describing Chertoff's case for greater surveillance by governments to hundreds of privacy advocates as a "confrontational challenge."

"... His vision of a broad surveillance society – supported by massive databases of biometric data collected from hundreds of millions of people – presented a chilling future. Rather than *terra incognita*, Chertoff seemed to say there is a known reality about our future course and there is little that the privacy community can do about it," Geist wrote in his popular blog.

Hopefully, Chertoff's comments will serve as inspiration for privacy advocates to make an even stronger case for privacy rights in the post 9-11 world.

The conference program underscored the wide range of issues which will have an impact on privacy in the coming years as well as the increasingly global nature of privacy issues.

We prepared 14 workbooks before the conference. Most included a commissioned paper by a subject-matter expert and a variety of other resources, such as bibliographical materials, to satisfy the curiosity of participants who might be new to a particular subject, as well as the more rigorous requirements of key policy and decision-makers to locate trustworthy information about the privacy implications of our conference topics. These are available on our conference website at [www.privacyconference2007.gc.ca](http://www.privacyconference2007.gc.ca) and are an important legacy of the conference.

We have posted details about the cost of the conference on our website. We stayed well within our overall financial targets.

Feedback from conference participants was extremely positive. In fact, one of the few frustrations expressed by delegates was that there were too many sessions of interest occurring at the same time!

## **A Global Concern**

The impact of globalization on privacy is a growing preoccupation of my Office. The fact that more and more personal information is crossing borders means data breaches often affect people in multiple countries – as we saw in the TJX/Winners case. The increasing popularity of the Internet also raises many cross-border issues with implications for our Office.

I am pleased to report we are making progress in our work with international counterparts to find global privacy solutions.

Resolutions adopted during the conference by data protection authorities from every continent recognized the increasingly global context of privacy issues.

Commissioners called for international standards for the use and disclosure of personal information collected by travel carriers about passengers. They warned that the transfer of personal information from travel agents, carriers and domestic and foreign governments poses an ongoing threat to the personal privacy of passengers. A global solution needs to be developed with the cooperation of carriers, law enforcement agencies, international organizations, civil liberties groups, and data protection and privacy experts.

Data protection authorities adopted two other resolutions: to improve international cooperation; and to build upon the work of the International Standards Organization to establish shared privacy standards in the area of information technology.

My Office has also been working on transborder issues as part of other international initiatives.

## **OECD/APEC Efforts**

I was pleased to chair an Organisation for Economic Co-operation and Development (OECD) volunteer group examining ways to encourage cooperation between data protection authorities and other enforcement bodies with respect to cross-border complaints and cases arising from transborder data flows.

The group produced a report summarizing the powers of enforcement authorities in OECD member countries and their ability to share information to facilitate cross-border cooperation. The report concluded that, despite differences in national laws, there is considerable scope for a more global and systematic approach to cross-border privacy law enforcement cooperation. In June 2007, the OECD adopted a recommendation on cross-border cooperation which was based on the work of the volunteer group.

The volunteer group's work will also be highlighted during a June 2008 OECD ministerial meeting in Korea, where the theme will be the future of the Internet economy.

My Office has also contributed to the work of the Asia-Pacific Economic Cooperation (APEC) on privacy issues.

Canada has been active in ensuring that core privacy values and principles are reflected in APEC data protection rules – an initiative that will be of clear benefit to Canadians given our increasing data flows with APEC member countries. Our work in 2007 focused on exploring ways to implement an APEC Privacy Framework.

## **PIPEDA Reform**

Here at home, we supported the work of a committee of MPs reviewing *PIPEDA*. Members of the House of Commons Standing Committee on Access to Information, Privacy and Ethics presented the federal government with 25 recommendations for fine-tuning *PIPEDA*. The recommendation which received the most attention was a call for mandatory data breach notification – a concept I strongly support.

In response, the federal government launched public consultations on *PIPEDA* reform late in the year, requesting input on the parameters of data breach notification and other issues.

We appreciate these consultations and look forward to seeing changes to improve *PIPEDA* – and ensure even stronger privacy protection for Canadians.

## **Welcoming an Assistant Commissioner**

I am very pleased that Elizabeth Denham, our new Assistant Privacy Commissioner, will help lead the search for innovative solutions to the significant privacy challenges Canada will be facing in the coming years.

Before her appointment, Ms. Denham was Director of Research, Analysis and Stakeholder Relations in our Office. Previously, she had been the Director, Private Sector, in the Office of the Information and Privacy Commissioner of Alberta.

Ms. Denham's experience in developing relationships with stakeholders, her perspective formed by her work with provincial commissioners and her extensive expertise in the privacy field will undoubtedly be of enormous benefit to the OPC in the coming years. She will be responsible for *PIPEDA*, working alongside Raymond D'Aoust, Assistant Commissioner responsible for the *Privacy Act*.

## **A Dedicated and Expert Team**

I would also like to acknowledge the very hard work of the dedicated team in my Office over this past year. Hosting a major international conference was a huge undertaking – on top of an already intense workload. I am also pleased that our Office is attracting a new generation of personal information experts.

I offer my sincere thanks to all the employees of the Office of the Privacy Commissioner for their immense contribution to protecting the privacy rights of Canadians.

**Jennifer Stoddart**  
**Privacy Commissioner of Canada**

## PRIVACY BY THE NUMBERS IN 2007

---

Average number of <i>PIPEDA</i> inquiries per month:	538
Average number of <i>PIPEDA</i> complaints received per month:	28
Average number of <i>PIPEDA</i> investigations closed per month:	33
Total investigations closed during the year:	420
Parliamentary appearances:	7
Number of bills/acts reviewed for privacy implications:	15
Research activities commissioned:	19
Speeches and presentations delivered:	92
Media requests:	474
Interviews provided:	301
News releases issued:	44
Publications distributed:	2,043
Average hits to our website per month from Canada:	39,429
Average hits to our website per month from other countries:	86,155
Average hits to our blog per month:	14,173
Legal opinions prepared:	82
Litigation decisions on <i>PIPEDA</i> cases rendered:	3
Litigation cases settled:	5
<i>Access to Information Act</i> requests received and closed between April 2007, when we first became subject to the legislation, and the end of the calendar year (all within prescribed timelines):	21
<i>Privacy Act</i> requests received and closed during the same period:	14





## NEW STRATEGIC PRIORITIES

---

The constantly changing world of privacy issues means our Office must find ways to focus our efforts. In 2007 we identified four new strategic priorities which we believe represent some of the most significant threats to the privacy of people across Canada.

These priorities – information technology; identity management; national security; and genetic information – will help guide our policy, research and investigative work over the next three years.

### **Information Technology**

Information technology was an obvious choice for our list because virtually every current privacy issue and privacy complaint we receive contains an IT component.

Information and communications technologies have become integral to our daily lives. Technological advances mean more and more personal information can be gathered, stored, analysed and potentially accessed from anywhere in the world.

These developments provide undeniable benefits in terms of convenience and efficiency, but also carry great risks for privacy. Governments and businesses can now collect and use personal data on a scale that was until recently unimaginable.

Our Office will continue to develop the capacity to assess the privacy impact of new technologies. We will also work to help Canadians understand and, where possible, mitigate those privacy impacts.

We demonstrated in 2007 how our Office can make a difference in this area after identifying privacy concerns stemming from the integration of street-level photography with web-based mapping technology. This type of photography involves the use of high-resolution video cameras, often affixed to vehicles as they drive along city streets. The images – including images of people who may be identified – are then made available on the Internet.

It has become something of an Internet sport to find pictures of people captured in embarrassing or personal moments – a man leaving an adult video store or young women sunbathing, for example – and then share them on websites.

Google's Street View is one of several services that have been rolled out. To date, Street View has produced photographs taken in U.S. cities. We were concerned that street level photography, as currently deployed in the U.S., may not meet the basic requirements of privacy laws here in Canada. I wrote to Google outlining these concerns and we have received assurances from Google officials that they will ensure Street View will be compliant with Canadian legislation if it is deployed in Canada.

## **Identity Management**

The issue of identity integrity and protection stems from the fact that massive amounts of data are continually circulating.

Personal information has become a hot commodity, not only for legitimate organizations, but for criminals as well. We have seen an explosion of identity theft in recent years – a crime which carries both economic and emotional costs.

Improving personal information management practices can go a long way to reducing the possibility data will make its way into the hands of identity thieves. Our goal is to increase awareness of the importance of handling personal information with great care. Our public education efforts will be aimed at both organizations and individuals.

An important focus will be on the online world, where personal information is increasingly dispersed across commercial sites, social networks and personal blogs. People are finding the personal information they've posted online being used in ways they never imagined. In some cases, entire profiles – name, photo and other personal details – have been hijacked by impostors. We are developing tools to help people manage their online identity.

## **National Security**

National security measures introduced in the wake of the attacks of Sept. 11, 2001 have transformed the privacy landscape in Canada and around the world.

Too often, these measures have focused on the collection and sharing of personal information with little oversight and scant consideration of privacy and other individual rights. A growing list of private-sector organizations – airlines, banks and accounting firms, for example – have been deputized to collect personal information for the state.

The way we address security needs to reflect our society's fundamental values – including the right to privacy. We must constantly ask ourselves why we accept the growing shift towards security at the expense of privacy. Is it always justified? Is it irreversible?

These are messages we will continue to press as we work to ensure that national security initiatives adequately protect privacy.

## **Genetic information**

Advances in genetics are creating an array of new and complex challenges for privacy protection.

Interest in obtaining genetic information is increasing swiftly. Genetic testing for employment, criminal matters, research, medical care, access to insurance and to determine family relationships all raise significant and deeply sensitive privacy issues.

There's a need to increase public awareness about how genetic information can be used. We must also explore some of the new challenges for protecting privacy in a world where our genes reveal so much about us.





## KEY ACCOMPLISHMENTS IN 2007

---

### Proactively Supporting Parliament

- Appeared before parliamentary committees on issues such as identity theft and amendments to the *Canada Elections Act*.
- Worked with the Standing Committee on Access to Information, Privacy and Ethics on the statutory review of *PIPEDA*; responded to Industry Canada's consultation on *PIPEDA* review.
- Joined provincial and territorial counterparts in passing a resolution calling on the federal government to suspend its new no-fly list program until it can be overhauled to ensure strong privacy protections for Canadians.

### Serving Canadians

- Responded to more than 7,500 *PIPEDA*-related inquiries.
- Investigated hundreds of privacy complaints in the public and private sectors.
- Created a blog to help build links and stimulate discussion on privacy issues of interest to Canadians.
- Began work on a social marketing campaign aimed at encouraging awareness and prompting action on children's privacy online.
- Appeared in numerous court cases in order to help develop privacy-conscious jurisprudence in Canada.

## Supporting Business

- Launched an e-learning tool to help retailers ensure their privacy practices and policies meet their legal obligations and provide customers with the privacy protections guaranteed under *PIPEDA*.
- Published guidelines to help organizations take the right steps after a privacy breach, including notifying people at risk of harm after their information has been stolen, lost or mistakenly disclosed.
- Initiated a regional outreach program to extend and tailor compliance education to small and medium-sized businesses.

## Global Initiatives

- Hosted the largest-ever International Conference of Data Protection and Privacy Commissioners, honouring a 2002 commitment.
- Chaired an OECD group working to enhance cooperation between data protection authorities and other privacy rights enforcement agencies around the world. OECD adopted a recommendation on cross-border cooperation which was based on the work of the volunteer group.
- Contributed to an APEC data privacy group's efforts to implement a new privacy framework for APEC member countries.
- Worked with the Standards Council of Canada on the development of international privacy standards.
- Joined the International Standards Organization (ISO) and became a member of an important ISO Working Group tasked with developing and maintaining standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data.
- Participated in the International Working Group on Data Protection in Telecommunications, which has recently focused on Internet privacy.
- Played a lead role in the creation of an international association of data protection authorities and other enforcement agencies from francophone states.
- Became a member of the Asia Pacific Privacy Authorities Forum

## Other Highlights

- Prepared a submission and appeared before the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.
- Provided research grants to eight organizations through our contributions program – bringing the total funding provided for privacy research projects under the program over the last four years to over \$1 million.
- Co-hosted an Internet Privacy Symposium with the University of Ottawa's Law and Technology Group to explore new threats to online privacy, emerging trends and ways to better protect personal information in the future.
- Hosted a conference for investigators in Winnipeg in February 2007. The conference was attended by 56 investigators from our Office and 11 provincial and territorial offices.



## KEY ISSUE: DATA BREACHES

---

### Gambling with Personal Information

*2007 was a year of data privacy disasters, highlighting the need for companies to recognize the value of personal information and take more care in securing it*

Not so long ago, a group of executives was debating the merits of delaying an upgrade of their company's out-of-date computer security system.

One of them cautioned his colleagues in an e-mail:

*"It must be a risk we are willing to take for the sake of saving money and hoping we do not get compromised."*

Those words were prescient.

They were written by a vice-president at TJX – a name which has become synonymous with data breach. The e-mail was released during legal proceedings against TJX.

In fact, hackers had already broken into the international discount retailer's computer system and were busy pilfering the personal information of people who had shopped at Winners, HomeSense and other TJX-owned stores. The company's obsolete encryption technology was not up to the job of protecting this sensitive data.

TJX was one of many companies gambling with Canadians' personal information.

Too often, large corporations underestimate both the value of personal information and the risk that thieves will target it. As a result, we see deficient safeguards, lackadaisical privacy and security policies and procedures – and, of course, data spills.

The size of the worst of the data breaches we saw in 2007 was staggering.

Some 94 million debit and credit card numbers belonging to people in several countries were affected by the TJX intrusion – the largest personal information breach on record.



In a case in the United Kingdom, an official at Her Majesty's Revenue and Customs department ignored security procedures and put two discs containing the personal details of 25 million child benefit recipients into an envelope, which was then mailed through an internal post system. The discs failed to reach the addressee at another government department.

Here in Canada, a hard drive belonging to a CIBC subsidiary vanished – along with the personal information of close to half a million clients.

Of course, not all of the data compromised in these kinds of breaches winds up in the hands of criminals.

However, it is clear crooks have recognized that personal data is a goldmine. Identity theft is rampant – and lucrative.

---

NOTE: Information on data breaches voluntarily reported to our Office in 2007 is provided on page 39.

Businesses recognize the value of personal information to themselves – for targeted marketing campaigns, for example. Unfortunately, this perception doesn't always translate into security measures up to the job of protecting the information from criminals.

Just before the TJX breach became public, for example, Visa USA revealed that a little over a third of the very biggest retailers in that country were complying with the industry security standard. The figure for other large merchants was even worse – just 15 per cent.

We understand the picture in both the U.S. and Canada has been improving in the wake of TJX. Visa Canada has told us that virtually all major retailers were well on their way to compliance with the payment card industry data security standard.

One word – TJX – is no doubt going a long way when security experts ask senior executives for money to pay for upgrades.

All organizations must use strong security to protect personal information. It is not good enough to offer the excuse that, "We were moving as slowly as other companies."

Good security is expensive, but it is significantly less expensive than mopping up after a major data spill. Security experts have calculated that recovering from a significant data breach costs several times more than installing adequate safeguards in the first place.

Good privacy practices also go a long way to protecting personal information.

*PIPEDA* sets out 10 fair information principles that businesses must follow. These principles – sometimes called the “golden rules” of privacy – include such basics as seeking consent for the use of personal information; limiting the use, disclosure and retention of personal information; and using appropriate security safeguards.

The starting point for implementing these fair information principles is to critically examine the personal information being collected. Organizations should only collect personal information which is absolutely essential. After all, if you don't have this kind of information in the first place, it can't be lost or stolen.

A second critical step is to recognize the value of personal information which is collected and protect it properly.

By following this bottom-line advice, an organization should wind up with a relatively small and well-protected target.

The OPC has developed more detailed online training on how retailers can put fair information principles into practice. The e-learning course is available on our website.

Employee training is also critical to preventing data breaches. In many of the breach reports we receive from companies, the cause of the compromise is an employee's failure to follow company procedures.

For example, laptop theft is a common type of breach. We see employees leaving the office with laptops containing customers' sensitive personal information – contrary to company security policies.

Policies and procedures are only as good as the training that reinforces them.

Unfortunately, a survey of Canadian businesses conducted for our Office in 2007 found that only one third of them report having trained staff about their responsibilities under Canada's privacy laws. Larger businesses were the most likely to have provided training, with 63 per cent confirming they had done so.

Companies that have not trained employees who deal with personal information are exposing themselves to a significantly increased risk of a data breach. We hope to see more encouraging numbers the next time we conduct a survey on compliance with *PIPEDA*.

During 2007, we developed breach guidelines in consultation with industry and civil society groups. These guidelines outline key steps organizations should take after a breach, such as containing the breach, evaluating the associated risks, notifying the

people affected and preventing future breaches. The guidelines have also been adopted as a model in New Zealand. The Australian Privacy Commissioner is also proposing to adopt the guidelines.

We have been clear that voluntary guidelines do not take away from the need for breach notification legislation.

In fact, we have been urging the federal government to amend *PIPEDA* to add a notification requirement.

We believe mandatory notification will help protect personal information in two very important ways. First, it will provide an incentive for organizations to take privacy and security more seriously; and, second, it will give people the information they need to take measures to protect themselves against identity theft or other forms of fraud.

It is clear that people want this kind of information.

More than three-quarters of Canadians (77 per cent) believe government agencies and affected individuals should be notified if sensitive personal information is compromised as a result of a breach, according to a 2007 poll commissioned for our Office. Meanwhile, 66 per cent wanted to be notified if non-sensitive information was compromised.

One of *PIPEDA*'s tenets is that individuals should have control over their personal information. Breach notification offers people a choice. Individuals can decide for themselves how to respond to a breach. One person could decide that it would be a good idea to check her credit report more often. Another person may feel no action is warranted.

What's important is that the individual retains control.

Our Office believes breach notification is an important part of a comprehensive approach to reducing data breaches.

The TJX debacle, along with headlines about missing computer discs and hard drives as well as other lost data are a wake-up call for all organizations that collect personal information. These incidents starkly illustrate the need for companies to make both privacy and security a top priority.

When Canadians entrust their personal information to an organization, they expect – and the law requires – that this information will be well protected.

## A DATA BREACH INVESTIGATION

### THE TJX CASE: HOW HACKERS GAINED ACCESS TO 94 MILLION CREDIT AND DEBIT CARDS

The story of what has been called the “largest-ever online burglary” began one summer day in 2005.

It’s believed that thieves armed with an antenna and a laptop computer and some specialized software settled in outside a Marshall’s in Miami and broke into the store’s poorly protected wireless local area networks.

Once inside, they tapped their way into computer servers that process and store customer information from transactions for hundreds of stores owned by discount retail giant TJX, including Winners and HomeSense stores in Canada.

For the next year and a half, the thieves plundered the TJX computer system.

They ultimately gained access to at least 94 million credit and debit cards as well as the names, addresses and driver’s licence numbers of people who had returned merchandise at TJX stores.

The crime wasn’t particularly sophisticated. Detailed instructions on cracking the encryption protocol used to guard TJX’s wireless networks were readily available on the Internet.

It had been well established for some time that this encryption protocol – Wired Equivalent Privacy, or WEP – did not provide adequate network protection because it could be easily bypassed by someone with a bit of computer savvy.

TJX was aware of the concerns about its encryption protocol and was in the process of converting to a stronger technology at the time of the breach. In our view, the conversion was not done within a reasonable period of time.

The OPC’s investigation, conducted jointly with Alberta Information and Privacy Commissioner Frank Work, concluded TJX did not comply with either federal or Alberta privacy laws.

### KEY FAILINGS

The investigation highlighted a few critical failings:

1. TJX collected too much information and kept it for far too long.

The company should not have collected driver's licence and other identification numbers when merchandise was returned without a receipt. A driver's licence is proof someone is authorized to drive a car – not an identifier for analysing shopping-return habits. As well, a driver's license number is invaluable to identity thieves.

In response to our concerns, TJX proposed an innovative new process to deal with fraudulent returns. Information such as a driver's licence number will still be requested and keyed into the point-of-sale system, however, it will instantly be converted into a unique identifying number. This will allow tracking of unreceipted merchandise returns without keeping original identification numbers.

Prior to the breach, identification information collected from people returning goods was kept indefinitely.

Credit card information was also retained for a long time – some of the stolen information involved transactions dating back several years.

## **2. TJX failed to update its security systems in a timely way.**

TJX's process for converting to an up-to-date encryption protocol took two years to complete, during which time the breaches occurred. As a result, the company did not adhere to the requirements of the payment card industry's data security standard.

## **3. TJX did not adequately monitor its system for signs of an intrusion.**

The thieves were able to continue stealing data for a year and a half before TJX learned that suspicious software had been detected on a portion of its computer system. With proper monitoring, TJX should have detected the incident sooner.

## **LOOKING AHEAD**

TJX has complied with all of the OPC's recommendations on improving security, monitoring and other personal information management issues.

A year after it was discovered, the intrusion continued to have an impact.

Some legal proceedings against the company were ongoing. Investigations by the U.S. Federal Trade Commission, as well as an investigation by the Massachusetts Attorney General on behalf of a group of more than 30 state Attorneys General were continuing.

It's unclear how much the breach will wind up costing the company – but the total bill will certainly be in the hundreds of millions of dollars.



By the end of 2007, TJX had named a chief privacy officer and was advertising for a privacy director to develop and implement a comprehensive information privacy and security program.

---

### **How our Office Helps Organizations Prevent Breaches**

- We launched an online learning tool offering step-by-step guidance for retailers on how to protect customer information and meet *PIPEDA* obligations.
- We have published various online and printed materials on how businesses can safeguard personal information, including the booklet, *Your Privacy Responsibilities: A Guide for Businesses and Organizations*.
- We developed voluntary data breach guidelines in consultation with industry and consumer groups.
- We advise and assist organizations with their breach response actions, including advice on notification of affected individuals.
- We continue to press the federal government to make breach notification mandatory under *PIPEDA*, a move we believe would encourage businesses to improve security measures.
- We conduct audits of the personal information management practices of organizations covered by *PIPEDA* if we have reasonable grounds to believe the organization is contravening the legislation.
- Our investigations into privacy complaints help identify steps that businesses can take to better protect personal information.



## IMPROVING *PIPEDA*: A REVIEW OF OUR PRIVATE-SECTOR PRIVACY LAW

***A Parliamentary committee completed a mandatory review of PIPEDA in 2007 – an important step towards strengthening privacy protections for Canadians***

*PIPEDA*, along with its public-sector sister legislation, the *Privacy Act*, and provincial legislation provide the foundation for privacy protection in Canada.

The privacy landscape is constantly changing – and our laws need to keep up.

Consider how much the world has changed since a decade ago, when we began talking about what a private-sector privacy law in Canada should look like.

Back then, the Information Highway was a catchphrase; now it is a reality. The trickle of personal information crossing borders has become a torrent. Meanwhile, emerging technologies such as location tracking devices are raising new risks for privacy. And the fallout from 9-11 means governments are asking businesses for more information about our day-to-day lives.

It is critically important that *PIPEDA* remains capable of addressing all of these new challenges. The desperately out-of-date *Privacy Act* – left unchanged for a quarter-century – is evidence of the dangers of failing to modernize privacy legislation.

Fortunately, *PIPEDA*'s architects recognized the importance of regular updating. The legislation requires Parliament to review the part of the Act dealing with data protection every five years.

The House of Commons Standing Committee on Access to Information, Privacy and Ethics took on the task of conducting the first five-year review, beginning their work in the summer of 2006.

Committee members wrapped up public hearings on a wide range of issues in February 2007. They heard from 67 witnesses and considered 34 submissions from individual Canadians, private sector associations, privacy advocates and the Privacy Commissioner.

Overall, we feel the legislation has been well-received, that it is working reasonably well, and that we have most of the tools and powers we need to enforce the Act. The legislation offers Canadians strong privacy protections in the commercial sphere.

In our submissions to the committee, we noted the legislation has only been fully in force since 2004. While experience to date has been instructive, more time is needed before any major changes are made. The full impact of complex legislation takes time to unfold.

That said, some adjustments would be welcome to ensure privacy protections evolve with new trends and technologies.

In May 2007, the committee presented its final report, which included 25 recommendations for the government's consideration or further discussion.

Suggested amendments touched on a broad range of issues, including: business contact information; work product information such as physicians' prescribing patterns; employee-employer relationships; investigative bodies; witness statements; law enforcement and national security; individual or family exceptions; disclosure of personal information before transfer of businesses; added protection for minors; and mandatory data breach notification.

We deeply appreciate the effort of the Parliamentarians, researchers, organizations and citizens who contributed their experiences and expertise to the review process.

The Government of Canada tabled its response in October. In our view, a very significant element of the response was the acknowledgement that an increasingly global response is required to meet privacy threats. The data-processing industry has become increasingly international, and so too have data security risks.

Inter-governmental cooperation, information sharing between jurisdictions and attention to trends emerging in other parts of the world have all become vital strategic considerations as we work to protect the privacy of Canadians.

In October, Industry Canada issued a consultation notice seeking public input on how best to implement certain provisions of the Government response. Views on data breach notification provisions, and the concepts of "work product" and "lawful authority," were

given particular emphasis. As well, Industry Canada sought views on witness statements, minors' consent and investigative bodies.

As part of this round of consultations, the Privacy Commissioner asked the Minister of Industry to closely consider five issues which will significantly impact our work in the years to come:

- We continued to promote a 'contextual' approach to work product information.
- We supported a requirement for breach notification, and stressed the need for clear triggers and thresholds in any new *PIPEDA* provisions.
- We asked that the possibility of *PIPEDA* amendments governing access to documents covered by solicitor-client privilege be left open, pending a decision from the Supreme Court of Canada in *Privacy Commissioner of Canada v. Blood Tribe Department of Health*.
- We urged that any new provisions on privacy in the employer-employee context take Alberta and Quebec legislation into consideration in order to better recognize that the unequal bargaining power in employment relationships means employees may not feel in a position to withhold consent for the collection of their personal information. Our Office sees merit in Alberta's approach of a reasonable purposes-based employee code, combined with the notion in the Quebec Civil Code, which obligates employers to respect the dignity of workers.
- We asked for greater flexibility to refuse and/or discontinue complaints if their investigation would serve no useful purpose or are not in the public interest, thereby allowing us to focus investigative resources on issues of broader systemic interest.

The deadline for comments to Industry Canada was mid-January 2008. The department received 67 submissions and was reviewing those in early 2008.

We look forward to the next stage of the legislation's review and the important dialogue it serves to generate between privacy advocates, regulators, industry and Parliamentarians.





## COMPLAINT INVESTIGATIONS AND INQUIRIES

As Canadians become more knowledgeable about privacy issues, organizations are being challenged to fulfill their responsibilities with respect to personal information. In particular, consumers are increasingly aware of the serious ramifications of identity theft and, as a result, are more insistent that companies meet their obligations when collecting personal information.

People do not want sensitive information such as driver's licence numbers collected and retained without a legitimate reason, nor do they want their credit card numbers and expiry dates printed on receipts.

Many companies do take their privacy responsibilities seriously. But it is also clear – both from the complaints we receive and from the data breaches voluntarily reported to our Office – that many organizations could do more.

Businesses that handle personal information need to update their privacy policies and practices regularly. They must keep their data security up-to-date. And, they must also ensure that employees are kept informed of changes and receive regular training.

### Inquiries

Our Inquiries Unit responds to questions from individual Canadians, government institutions, private sector organizations and the legal community. Inquiries officers provide information on a broad range of issues under both *PIPEDA* and the *Privacy Act*.

We received 7,636 *PIPEDA*-related inquiries in 2007, a substantial increase from the 6,050 received a year earlier. We have noticed a marked increase in interest concerning identity theft and social networking sites such as Facebook.

### Complaints

We received 350 new *PIPEDA* complaints during 2007. We received 424 complaints in 2006; 400 in 2005; and 723 in 2004.

The year-over-year decrease in complaints is, in part, the result of a streamlined complaint-acceptance process introduced in 2007. Under this process, when an individual brings a complaint which is factually similar to complaints already under investigation, we inform the individual that the issue is already under investigation and will be addressed by the Commissioner in her findings. This approach is also used with complaints for which a finding has already been issued on a similar case.

In such cases, we offer complainants the option of referring to similar findings as a way to resolve the particular issues they may have with an organization.

By way of example, we currently have underway five investigations concerning drug testing for employment, while an additional 27 people agreed not to file official complaints about the same issue.

**NOTE:** Detailed information about complaints as well as findings and other dispositions are included in Appendix 1 of this report.

In some instances, although an individual's situation may be similar to that of another complaint, the facts may vary enough to warrant a full investigation.

Another possible reason for the decline in complaints is that organizations may be becoming more knowledgeable about their privacy obligations. Moreover, many now have internal complaint-resolution processes in place in order to resolve privacy issues with their customers. Our Inquiries Unit also advises individuals to attempt to resolve their disputes with organizations before they file a formal complaint with our Office.

## Complaints by Sector

As has been the case since 2004, when *PIPEDA* was fully implemented, the financial institutions sector was the sector most often targeted in our 2007 complaints. We received 105 complaints involving financial institutions in 2007. This represented almost a third of total *PIPEDA* complaints, which is similar to the proportion of complaints involving this sector over the last few years.

As in past years, the other major sectors for complaints were telecommunications, insurance, sales and transportation. We have, however, seen a decrease in complaints involving companies in these industries over the last few years.

We have seen a steady increase in complaints about professionals and the accommodation sector. However, the number of complaints against these sectors remains small in comparison to others.

With respect to complaints involving the insurance industry, we are seeing more issues involving the covert collection of personal information by private investigation firms.

*PIPEDA* includes provisions for designating a private investigation company as a “private investigative body” which carries specific responsibilities under the legislation.

We understand there may be a need for covert collection of personal information where other less privacy invasive efforts have failed. However, a key concern about this type of investigation is the risk that innocent third parties may be captured on covert video surveillance tapes. Few of us would like to be videotaped in a bathrobe on our front step simply because we happen to live next to someone under suspicion of insurance fraud.

We are working with both insurance and private investigation organizations to find a balance between their need to conduct their business and individuals’ right to privacy. Insurance companies and their contractors should conduct covert surveillance only as a last resort. Businesses should ensure that the decision to conduct covert surveillance is made at a senior level.

Part of the solution may be for insurance companies to establish detailed contracts with investigative firms to ensure that the parameters of surveillance are clearly spelled out. As well, investigative firms need to develop specific policies regarding surveillance, including the videotaping of third parties.

## Complaint Trends

Our Office closed 420 complaints in 2007. Of these, the vast majority (39 per cent) concerned use and disclosure issues, a trend which has continued from previous years. Also consistent with previous years, other common types of complaints were collection (19 per cent) and access (16 per cent).

Almost a third (30 per cent) of complaints closed in 2007 were settled during the course of an investigation. These are complaints for which the Office has negotiated an outcome which is satisfactory to all parties and no finding is issued. In 2004, we defined the “settled” category in order to track this outcome.

**Closed 2007 Complaints By Finding**

	Percentage
Settled	30
Discontinued	21
Not well-founded	15
Well-founded Resolved	15
Resolved	10
Early Resolution	3
No jurisdiction	3
Well-founded	2

In 2004, 40 per cent of our cases were settled. Since then, however, this percentage has steadily declined. The trend may be a reflection of the fact we are seeing more complex cases where an extensive investigation is required.

A significant number of closed cases were discontinued (21 per cent) by the complainant or our Office. This represents an increase over previous years. As in the past, some complainants decide for personal reasons to abandon their complaints. Others do not proceed because they have resolved the issue with the organization before the active investigation has begun. Still others drop their complaints because of lengthy treatment times. Sometimes our Office must discontinue complaints because complainants have not provided us with additional details which we have requested and are necessary to complete an investigation.

Following the completion of investigations, 15 per cent of all complaints were found to be not well-founded and that the organization had complied with *PIPEDA*. Another 15 per cent of complaints were well-founded and resolved. In other words, there was a violation of *PIPEDA*, but the respondent organization agreed to comply with our recommendations.

The determination of whether a fully investigated complaint is well-founded or is well-founded and resolved depends on the level of cooperation we receive from the respondent organization.

A finding that a complaint is well-founded is reached when the Commissioner is of the view there has likely been a contravention of *PIPEDA*. She makes recommendations in a preliminary report with respect to corrective actions the respondent should take. The respondent has 30 days to reply to the preliminary report.

Since this new preliminary report process was established in 2006, it has become an effective means of ensuring that organizations remain accountable.

If the respondent complies with the recommendations, a well-founded and resolved finding is usually reached. In cases where the respondent does not fully comply, the complaint is deemed to be well-founded.

We included preliminary reports in 38 closed complaints in 2007. Of these, 34 organizations complied with the Commissioner's recommendations.

In 2007, only four organizations chose not to implement our recommendations at the conclusion of an investigation. The Commissioner has consistently sought to have her recommendations upheld by the Federal Court in such cases.



As we prepared to publish this annual report, all four organizations that initially declined to adopt our recommendations had finally agreed to comply, either before or after we referred the matters to litigation.

## Treatment Times

The average treatment time (calculated from the date the complaint is received to the date the report of finding is mailed) for *PIPEDA* complaints closed in 2007 was 15.7 months – approximately the same as in 2006.

On a more positive note, there were only 44 files in abeyance – unassigned because no investigator is available – at the end of 2007. That's substantially lower than the 76 files in abeyance the previous year.

We are committed to reducing treatment times and eliminating the backlog of cases – without compromising quality. Our Office is actively pursuing innovative steps to that end.

Changes implemented in recent years, including the hiring and training of new staff, have helped revitalize our investigations unit. We plan to further improve service delivery by:

- Continuing to hire more staff;
- Increased automation and the use of technology in processing files; and
- Streamlining our investigation processes.

All of this work is essential to sustaining Canadians' renewed trust in our Office and in our ability to protect their privacy rights. Fair, prompt and effective treatment of complaints also provides a key opportunity for educating both the private sector and individual Canadians.

## Commissioner-Initiated Complaints

The Commissioner uses her powers to launch complaints on a wide range of privacy issues. Following are summaries of two significant Commissioner-initiated complaints closed in 2007:

### **SWIFT Case: Transborder data flows raise new privacy risks**

The Privacy Commissioner launched an investigation in August 2006 following newspaper reports that the Society for Worldwide Interbank Financial Telecommunication (SWIFT) had disclosed tens of thousands of records containing personal information to the U.S. Department of the Treasury.

The disclosed materials included personal information originating from, or transferred to Canadian financial institutions. This likely included such information as names, addresses, account numbers and amounts of transfers.

In Canada, SWIFT collects personal information from, and discloses it to, Canadian banks for cross-border payments, securities clearing and settlement, and treasury and trade services. Its presence in Canada is significant. The vast majority of international transfers involving personal information flowing to and from Canadian financial institutions use SWIFT's network.

Following an investigation, the Commissioner concluded in April 2007 that SWIFT was subject to *PIPEDA*, but had not contravened it.

The Commissioner noted that the legislation allows organizations such as SWIFT to abide by the legitimate laws of other countries in which it operates. She also noted that *PIPEDA*'s exception to knowledge or consent applies to an organization disclosing personal information when a lawful subpoena is issued.

In this case, the U.S. Department of the Treasury began issuing subpoenas to SWIFT for data held in its U.S.-based operating centre following the terrorist attacks of Sept. 11, 2001.

In her findings, the Commissioner noted that if U.S. authorities need to obtain information about financial transactions with a Canadian component, they should be encouraged to use existing information mechanisms that have some degree of transparency and built-in privacy protections, such as Canadian anti-money laundering and anti-terrorism financing mechanisms.

---

### **Telecommunications Case: Highlighting the importance of authentication**

Assistant Privacy Commissioner Raymond D'Aoust initiated complaints against three Canadian telecommunications companies following the publication of a November

2005 article in *Maclean's* describing how the magazine had obtained the Privacy Commissioner's telephone records.

The records were purchased from a U.S. data broker, Locatecell.com, which had obtained them from Bell, TELUS Mobility and Fido.

The investigation revealed that Locatecell.com had used "social engineering" to persuade phone company customer service representatives to divulge confidential information, either in the specific instances alleged and/or subsequent test cases. Social engineering involves manipulating people into divulging personal information, for example, by pretexting – pretending to be someone authorized to obtain the information.

The Assistant Commissioner concluded that the companies' authentication procedures and staff training were not sufficient to adequately protect customer information or meet *PIPEDA* requirements.

He was also concerned that the companies had not done enough to alert employees about the tactics used by data brokers – even though concerns had already been raised by incidents in the United States.

Although the Assistant Commissioner was pleased that all three companies revised their customer authentication procedures shortly after the disclosures came to light, he recommended further changes to staff training, procedures on authentication and disclosure of personal information.

The companies implemented all of these measures except one, for which they proposed other actions which the Assistant Commissioner found acceptable. As a result, he found the complaints well-founded and resolved.

The Assistant Commissioner noted that organizations must adapt their personal information management policies and practices as threats to personal information continue to emerge and evolve.

Initially, the Assistant Commissioner also opened a complaint against Locatecell.com., however, preliminary results of our inquiries revealed we lacked jurisdiction to continue the investigation.

Following these incidents and legal actions against data brokers in the United States, broker activities have either stopped or been drastically curtailed. Many broker websites are unavailable, and the Locatecell.com site has been inoperative for some time.

## CASES OF INTEREST

*The following represent a sample of cases we worked on in 2007 which have a systemic significance for privacy issues in Canada.*

---

### **Court decision prompts cross-border investigation**

A Federal Court decision in February 2007 set aside the Privacy Commissioner's decision that she lacked jurisdiction under *PIPEDA* to investigate a complaint against a U.S.-based data broker, Accusearch Inc., operating as Abika.com.

As a result of this decision, our Office is conducting an investigation of a complaint filed by an individual against Accusearch. As part of our investigation, we have contacted the U.S. Federal Trade Commission, and are actively discussing how we can work jointly on issues pertaining to Accusearch.

---

### **Credit card number printed on airline ticket**

When a travel agency customer purchased an airline ticket, he was upset to discover that his credit card information had been transferred to a travel wholesaler and that the full card number and expiry date were printed on his ticket.

The Commissioner recommended that the travel agent better inform customers of the fact their personal information would be transferred to wholesalers.

As well, the Commissioner recommended that the agency confirm the wholesaler's personal information handling practices, noting that – although there was a related contract between the two parties – the wholesaler was reluctant to reveal its practices.

The agency later informed our Office that it would no longer conduct business with the wholesaler.

Until the issuing of paper tickets ceased altogether (in December 2007), the Commissioner recommended that the agency explain to customers that credit card information would appear on paper tickets. Additionally, it must offer them the option of an e-ticket, which does not contain this information.

**Insurance officer discloses information without proper consent**

An individual complained that a medical insurance benefits administrator inappropriately disclosed sensitive personal information to his employer, despite the fact he had signed a limited consent form for information disclosure.

When the individual applied for long-term disability benefits, he had negotiated a restricted consent agreement with the insurance company adjudicator, with the express purpose of restricting the insurer's right to transfer medical information to his employer.

Months later, an insurance rehabilitation officer retained by his employer thought she had the complainant's verbal consent to tell his employer that he was ready to return to work.

In doing so, she e-mailed to his employer excerpts of a medical specialist's report – even though the complainant had reminded her of the limited consent instructions.

The Privacy Commissioner concluded the disclosure was inappropriate and written consent ought to have been obtained. The Commissioner recommended that the company update its policies and training. The company followed these recommendations.

---

**Telecommunications company fails to obtain consent to record calls**

An individual complained that a telecommunications company was not obtaining proper consent before recording its outgoing calls.

The company had called the complainant's mother, but had not informed her that the call was being recorded. The company's policy required employees to notify individuals of the recording of incoming calls, but not outgoing calls.

According to the company, a statement in its written privacy policy was a sufficient means for obtaining consent for the recording of outgoing calls; however, the Privacy Commissioner disagreed.

She recommended the company inform customers at the beginning of each outgoing marketing call that the conversation would be recorded or otherwise monitored. Customers should also be informed of the reason for doing so.

The telecommunications company agreed to implement the recommendations.

---



### **TV station takes steps to secretly record employee calls**

A union representing employees of a television station in a small community alleged that a manager had installed telephone-call recording equipment at a customer service representative's work station and had taped her telephone conversations without her knowledge and consent.

The investigation confirmed the allegation. We retrieved a recorded conversation between the employee and her husband from a file in the complainant's computer. The complainant told us she had not been aware that the call was being recorded.

When questioned, the employer claimed the equipment was not yet working and that it had been installed on a test basis, with the intent of recording conversations in case of a billing dispute and also to deter abusive customers.

The Assistant Commissioner recommended that, since the station intended to install equipment at all customer service representatives' work stations, it must inform employees of its plans and their purpose beforehand. It was also required to inform customers that their calls may be recorded and why this was being done.

The complaint was considered well-founded and resolved. The station ultimately decided not to record calls.

---

### **Contest rules adequately warned about sharing of e-mail addresses**

A subscriber to a company's e-newsletter entered its contest to win a vacation for four people. He provided e-mail addresses of other individuals so that he could receive additional contest entries.

However, he was dismayed when he discovered that the e-mails the company sent to those other individuals were designed to appear as though they came from him. In particular, he was upset that his ex-wife had received an email in which he purportedly suggested the two of them travel together if he won the contest.

He complained his name had been used in the e-mails without his consent.

The Assistant Privacy Commissioner concluded the complaint was not well-founded. The contest rules and wording were clear that e-mail messages to referrals would be personalized as though the contestant had sent them. Given that the prize was a trip for

four, she thought it reasonable to expect the message could include a suggestion that the subscriber and e-mail recipient travel together.

## **Incident Investigations**

Our Office also conducts investigations of incidents that relate to possible contraventions of *PIPEDA*. Reports of incidents are received through self-reporting by organizations; media reports on possible breaches; and information received from individuals who would like an issue to be addressed, but are not necessarily directly affected.

Examples of incidents include issues such as credit card receipts found in dumpsters or reports of information breaches on websites.

When an incident comes to our attention, we work with the responsible organization to correct any deficiencies and resolve outstanding matters such as notifying affected customers; retrieving information; and ensuring appropriate safeguards are implemented.

In 2007, we conducted 12 investigations into incidents brought to our attention from a source other than the organization directly involved in the incident.

## **Self-reported Data Breaches**

Despite the fact that privacy legislation has been in place for a number of years, not all organizations have clear policies and procedures regarding data breaches. That said, we believe there is a heightened awareness of the need to alert our Office of privacy breaches and also to notify affected customers – in part stemming from the development and publication of our breach guidelines.

Organizations voluntarily reported 34 breaches to us in 2007, up from 20 reports the previous year. The self-reported data breaches in 2007 compromised the personal information of some 50,000 people.

Although we began to see reports of breaches from different sectors, including research groups and advertising companies, the bulk of these reports continued to flow from the banking, telecommunications and retail industries.

Of particular note is the fact that half of the breaches reported to us related to electronically stored data – often customer information stored on laptop computers that had been stolen. As well, we found that almost nine in 10 people affected by a self-reported breach were put at risk because their personal information was held in an

electronic format that was either not secured or lacked adequate protection mechanisms such as firewalls and encryption.

We were pleased to note that organizations voluntarily reporting to us did so in a timely way – often within a day or two of the incident. Prompt notification helps us in preparing for media inquiries or complaints that follow notification of affected individuals. Self-reporting also allows us to gather statistics and educate organizations and the public on the causes of data breaches as well as recommended preventive measures.

Brief descriptions of some of the breaches reported to our Office in 2007:

- A laptop being used by the employee of a firm under contract to a financial institution was stolen from the employee's home. The laptop contained the personal information of several hundred employees, but was not considered sensitive. Both the financial institution and the firm under contract had appropriate controls in place to protect personal information, but the employee had not followed them. As a result of this incident, the institution implemented additional controls such as encryption software.
- A laptop containing customer records was stolen from a vehicle belonging to a financial services company employee. More than half of these records included social insurance and account numbers. The company notified individuals and placed alerts on the accounts of affected customers.
- The laptop of an employee of an agency promoting a casino event was stolen from a car. The laptop contained a password-protected database of information on some event participants, but the data was not encrypted. The personal information included participants' names and ages, contact information, driver's licence numbers and, in one case, passport and health card numbers. Following the incident, the agency notified affected individuals and offered credit monitoring. It also introduced several security measures, such as encryption software on laptops and also reminded employees of security policies and procedures. The employee responsible for the breach was relieved of his duties.

We hope the growing awareness about the need to alert our Office and affected individuals about privacy breaches will soon translate into more effective security measures. We continue to urge individuals and organizations to take basic data security precautions such as:

- Limit the amount of personal information collected, used and carried on electronic devices;

- Never leave a laptop unattended where it could be stolen;
- Use technologies which enhance security and privacy such as data encryption and anonymizing services;
- Use hard-to-crack passwords;
- Avoid automatic login features which save user names and passwords; and
- Ensure that personal information is completely overwritten – not just deleted – from a hard drive before discarding or selling a computer.

By following these steps, organizations can significantly reduce the risk that the personal information they hold will be compromised.





## AUDIT AND REVIEW

---

Audits are one of the compliance tools provided under *PIPEDA*. The Privacy Commissioner has the power to audit an organization's personal information practices where she has reasonable grounds to believe there is non-compliance with the Act.

Once an audit is initiated under *PIPEDA*, the auditor has the delegated authority to receive evidence from witnesses; may enter premises at any reasonable time; and may examine or obtain copies of records found on the premises. Where necessary, the Privacy Commissioner may compel individuals to provide evidence.

After an audit is complete, we provide the organization with a report on our findings and any recommendations the Commissioner considers appropriate. The report may be disclosed in the public interest.

Our Office also conducts audits of federal government institutions subject to the *Privacy Act*.

The goal of audits – both in the private and public sector – is to promote accountability and compliance with applicable legislation, policies and standards, and also to contribute to the improvement of privacy systems and practices.

### **A framework for initiating audits under *PIPEDA***

One of the most frequently asked questions from organizations subject to *PIPEDA* might be: How do you decide whether or not to conduct an audit?

A decision to audit or not to audit is made on a case by case basis. To conduct an audit, the law requires the Commissioner to have reasonable grounds that there is non-compliance with the Act.

In 2007, we developed a framework for initiating audits which provides some insight into the audit selection process.

## How do we decide whether or not to conduct an audit under *PIPEDA*

### Strategic Plans

The Office's Strategic Plan and annual Report on Plans and Priorities describe the results we wish to achieve. Throughout the process of deciding whether or not to audit, consideration is given to the Commissioner's mandate, goals, plans and priorities.

#### Issue Analysis

**PRINCIPLE 1:** Do factors exist, or have events occurred, which indicate a risk of noncompliance with The Act and/or the absence of sound privacy management practices?

This process involves the identification, analysis and validation of potential privacy issues associated with an industry, entity or program, and where possible, a preliminary review of the area's major privacy management control functions. Issue analysis is generally conducted internally using information collected by the OPC through investigations and/or research, but may involve several interventions, including enquiries with management. Factors indicating the absence of sound privacy management practices may include, but are not limited to: credible media reports, the recommendations of parliamentary committees, contraventions revealed through whistleblowing, incident investigations, the results of complaint investigations, entity or industry requests for review, the results of empirical studies or industry polls, other.

#### Grounds

**PRINCIPLE 2:** Does sufficient and credible evidence exist to support a serious possibility that an audit would disclose an ongoing contravention of the Act?

Reasonable grounds testing involves the examination of information gathered during issue analysis activities, and the assessment of whether there are sufficient grounds to support the Commissioner's use of discretionary authority under section 18(1) of the Act. Internally, the OPC establishes a clear basis for audit and ensures that a sound evidentiary threshold is used in arriving at such a determination.

#### Action

**PRINCIPLE 3:** Given the results of issue analysis and reasonable grounds determination, what measures would best promote and encourage compliance and the use of sound privacy management practices? Is the area under consideration best addressed through an audit and is it amenable to audit?

Our Office recognizes that no single tool or instrument will best ensure compliance in all situations. For that reason, the Commissioner considers all means available, including audit, to encourage compliance and promote sound privacy management practices. The final decision to audit would be subject to numerous considerations not limited to: the nature of the case, the significance of systemic risks, the frequency with which the issue has been identified, the extent to which remedial action has been taken, the results and findings of completed or ongoing privacy investigations and previous Office positions.

A record setting out the basis upon which the Commissioner's decision to initiate an audit is made.

## Audits of Equifax and TransUnion

The Privacy Commissioner concluded concurrent audits of the online identification and authentication systems of credit reporting bureaus Equifax Canada and TransUnion.

Equifax initiated legal proceedings challenging the existence of reasonable grounds justifying the Privacy Commissioner's decision to audit. Notwithstanding the position maintained by Equifax throughout the process that the audit was not based on reasonable grounds, the audit was concluded. A report was provided to Equifax and no further steps were required to be taken by Equifax with regard to this audit.

TransUnion also took the position that the Commissioner lacked reasonable grounds, but chose not to take legal action. As was the case in the audit of Equifax, a report was provided to TransUnion and no further steps were required to be taken by TransUnion with regard to this audit.

## Self-assessment tool

Our Office is preparing a tool to assist organizations in assessing their compliance with *PIPEDA* and its fair information principles. This tool will help organizations diagnose problems with their privacy systems and practices.

We are seeking comments on this new self-assessment tool from a number of chief privacy officers of large businesses; academics; leaders in management development and training; as well as business and professional associations.

We expect to have a final version available for medium- and large-sized organizations in 2008.



## IN THE COURTS

---

The Privacy Commissioner may initiate court action where an organization refuses to adopt her recommendations in well-founded cases, which has helped establish a high level of compliance with recommendations.

Under section 14 of *PIPEDA*, a complainant or the Privacy Commissioner may, in certain circumstances, apply to the Federal Court for a hearing in respect of any matter referred to in the Commissioner's report.

Section 15 also allows the Privacy Commissioner, with the consent of the complainant, to apply directly to the Federal Court for a hearing in respect of any matter covered by section 14. This section also allows the Commissioner to appear before the Federal Court on behalf of any complainant who has applied for a hearing under section 14; or, with the permission of the Federal Court, to appear as a party to any section 14 hearing not initiated by the Commissioner.

Since we reported on the status of ongoing court cases in our 2006 *PIPEDA* annual report, new applications have been filed and some ongoing litigation has been settled. These new developments are discussed below.

In keeping with the spirit and intent of our mandate, we have respected the privacy of individual complainants by not including their names.

### Settled Cases

In 2007, a number of court applications filed against organizations were settled prior to being heard and determined by the Federal Court.



---

*X. v. ING Canada Inc.*

Federal Court File No. T-1283-07

---

A complainant brought an application for judicial review under section 18.1 of the *Federal Courts Act*. The OPC initiated a mediation process, and following a negotiated settlement, the application was discontinued by the complainant.

---

*X. v. Brampton Flying Club*

Federal Court File No. T-192-05

---

A complainant filed an application under section 14 regarding allegations that the Brampton Flying Club failed to provide access to his personal information within 30 days of his written request and tried to charge him an unreasonable amount to answer his request. This case was settled by the parties in January 2007.

---

*X. v. Laidlaw Transit Ltd.*

Federal Court File No. T-684-07

---

An individual filed a section 14 application challenging a form of workplace surveillance that Laidlaw Transit Ltd. had undertaken. The OPC helped mediate the dispute. The individual discontinued the application and the parties reached a settlement.

---

*X. v. The Bank of Nova Scotia*

Federal Court File No. T-2126-05

---

This case concerned a complaint that one or more employees of the Bank of Nova Scotia obtained personal information without consent and shared the information with a third party. The application filed by the complainant in the Federal Court was discontinued by the complainant and settled between the parties.

---

*Privacy Commissioner of Canada v. Air Canada*

Federal Court File No. T-342-07

---

The Privacy Commissioner filed a Federal Court application against Air Canada to have its recommendations implemented in a case dealing with the extent of personal health information collected by the organization to satisfy itself of an employee's ability to return to work.

The parties settled the dispute. Air Canada implemented the Commissioner's recommendations to our satisfaction.

## Ongoing Litigation

Ongoing litigation continued in respect of judicial review applications under section 18.1 of the *Federal Courts Act* and complainant-initiated court applications filed under section 14 of *PIPEDA* in which the OPC was involved as an added party or as an intervenor.

In one noteworthy case, State Farm Mutual Automobile Insurance Company questioned the Privacy Commissioner's jurisdiction to investigate a refusal to provide access to personal information and power to compel the production of documents during the course of an investigation.

In July 2007, State Farm filed an application in the Court of Queen's Bench of New Brunswick for a declaration that:

- *PIPEDA* did not apply to the disclosure of personal information sought by an individual complainant;
- *PIPEDA* was enacted outside the powers allotted to the federal Parliament;
- The Privacy Commissioner did not have the authority to investigate the complaint in question; and
- The Privacy Commissioner did not have the authority to compel production of the information sought.

The Privacy Commissioner filed a preliminary motion to have State Farm's application dismissed or stayed on the ground that the Federal Court was the more appropriate forum.

The motion was granted in January 2008 on the basis that the Federal Court was the more appropriate forum to determine the application, which involved questions of constitutional validity and the judicial review of the Privacy Commissioner's authority. State Farm's appeal from this decision will be heard in early 2008. Further developments will be reported in our next annual report.

Other significant court decisions rendered in 2007 are set out below.

***Judicial review applications under section 18.1 of the Federal Courts Act***

*Blood Tribe Department of Health v. The Privacy Commissioner of Canada et al.*

Supreme Court of Canada File No. 31755

---

Details of this ongoing matter have been reported in our last three annual reports. At issue is solicitor-client privilege and our ability to obtain the information we need to conduct our investigations. The final outcome – yet to come – will have profound implications for how we conduct our investigations.

The case began when a woman dismissed from her job with the Blood Tribe Department of Health asked for her personnel file and was denied access.

The woman filed a complaint with our Office. As part of our investigation, we asked for a copy of the woman's personnel file. The Blood Tribe Department of Health provided some records, but claimed solicitor-client privilege over other documents and refused to provide them.

Our position is that we need these documents in order to independently verify the claim that personal information being sought by a complainant is exempt from disclosure on the basis that it is information over which a claim of solicitor-client privilege has been made.

We issued an order that the organization produce the records. The Blood Tribe Department of Health went to court to challenge the Privacy Commissioner's jurisdiction to issue this order – bringing the investigation to a halt.

The Federal Court dismissed the Blood Tribe Department of Health's judicial review application.

However, the Federal Court of Appeal set aside the Privacy Commissioner's order, finding that language in *PIPEDA* is not clear enough to grant the Commissioner specific power to order the production of solicitor-client privileged documents. The Court proposed that we apply on a case-by-case basis to the Federal Court to examine claims of solicitor-client privilege in the context of complaints involving refused access to personal information.

We appealed from that decision to the Supreme Court of Canada, which scheduled a hearing for February 21, 2008.

The Privacy Commissioner has said she plans to revisit the issue with the Minister of Industry should amendments to *PIPEDA* be needed as a result of the Supreme Court decision.

---

*X. v. Accusearch Inc., dba Abika.com et al*  
Federal Court File No. T-2228-05

---

An individual filed a judicial review application seeking an order quashing or setting aside the Assistant Privacy Commissioner's decision that she lacked jurisdiction to investigate a complaint against Accusearch Inc., a U.S.-based organization operating as Abika.com.

Note: This case was also reported in our 2006 annual report.

The individual sought to review the Assistant Privacy Commissioner's position that she did not have jurisdiction to investigate. In February 2007, the Federal Court allowed the application on the grounds that the Assistant Commissioner did have jurisdiction to investigate the transborder flow of personal information in this case.

This was an important decision for our Office in that it helped strengthen our international outreach activities in order to better protect the personal information of Canadians.

As a result of the decision, we are conducting an investigation into the complaint about Accusearch.

As well, proceedings have been initiated in the United States against Accusearch with respect to its advertising and selling of confidential consumer telephone records to third parties without the consent of the individual concerned. Given our Office's increasing interest in international activities in helping to protect the personal information of Canadians, our Office is closely monitoring these proceedings.

---

***Complainant-initiated court applications under section 14 of PIPEDA***

*Dr. Jeffrey Wyndowe (Psychiatric Assessment Services Inc.) v. X.*  
Federal Court of Appeal File No. A-551-06

---

This is a long-running case, which was also discussed in our 2005 and 2006 annual reports. At issue is whether an individual has the right to access his personal information contained in notes taken by a physician conducting an independent medical examination on behalf of an insurance company.

The Federal Court considered whether such notes contained the "personal information" of the individual examined, and if so, whether any exemptions to refusing access to such information under *PIPEDA* applied. The Federal Court held the notes did contain the individual's personal information and that the claimed *PIPEDA* exemptions did not apply. Accordingly, it ordered the doctor to provide access to the notes.

The physician appealed. At the Federal Court of Appeal, the issues became, first, whether the notes constituted the personal information of the individual examined or the work product of the physician; and secondly, whether notes taken in the context of an independent medical examination occur in the course of a commercial activity covered by *PIPEDA*.

The Federal Court of Appeal issued its decision in February 2008 and held that:

- (i) Notes taken by a medical examiner in the course of an independent medical examination made at the request of an insurance company are taken in the “course of a commercial activity” and thus clearly subject to *PIPEDA*; and
- (ii) Notes taken by a medical examiner in the course of an independent medical examination clearly contain an individual’s personal health information, and, therefore, personal information.

The Federal Court of Appeal held that the individual has a right to access those portions of the notes which contain information he provided, and also to correct any mistakes in what the medical examiner may have noted about him.

However, the Court also concluded that information in the notes could be personal to both the individual and the physician, and that there may be need for a balancing exercise which takes into consideration the private interests of the individual and the physician, as well as the public interest in disclosure and non-disclosure.

The case was sent back to the Privacy Commissioner so that she, together with the doctor’s counsel, could determine which portions of the notes contain the individual’s “personal information” and should be released.

---

*X. v. Telus Communications Inc.*

Federal Court of Appeal File No. A-639-05

---

This case involved Telus employee complaints about the company’s implementation of a voice-recognition system.

In January 2007, the Federal Court of Appeal confirmed that:

- (i) The voice-print collected by Telus is personal information;

---

Note: This case was also reported in our 2004, 2005 and 2006 annual reports.



- (ii) On the facts, a reasonable person would find the introduction of voice-print technology for company authentication and security purposes to be reasonable in the circumstances;
- (iii) The Telus voice-print authentication system met *PIPEDA*'s consent requirement since employees could not be enrolled in the system without their active consent;
- (iv) None of the exceptions set out in section 7 of *PIPEDA* allowing for the non-consensual collection apply to these circumstances; and
- (v) Telus properly informed employees of the consequences which might arise if they refused consent.

---

*X. v. Scotia Capital Inc.*

Federal Court File No. T-2181-05

---

In response to the complainant's request for his personal information, Scotia Capital provided the complainant with a copy of his personal information but did not include his pay stubs or records of hours of work.

The complainant alleged Scotia Capital improperly relied on exemptions for third-party information and solicitor-client privileged materials. As a result of our investigation, the company forwarded additional information to the complainant.

The Assistant Commissioner concluded the organization was otherwise justified to withhold information which consisted of other individuals' personal information, or was subject to solicitor-client privilege.

The complainant filed an application in the Federal Court under section 14 of *PIPEDA*. The application was later dismissed.

---

*X. v. J.J. Barnicke Ltd.*

Federal Court File No. T-1349-06

---

An individual filed a complaint against J.J. Barnicke Ltd. alleging improper collection of personal information and inadequate policies to protect personal information. The company's vice-president had sent out a company-wide e-mail asking whether anyone knew which firm the complainant worked for.

The Assistant Privacy Commissioner concluded that, as there was no evidence that any J.J. Barnicke employee responded to the e-mail, there was no actual collection of

personal information. Therefore, the complaint regarding the improper collection of personal information was not well-founded.

However, the investigation revealed that J.J. Barnicke did not have appropriate privacy policies or procedures in place, nor was there a designated privacy officer accountable for compliance. Although J.J. Barnicke developed a privacy policy during the course of the investigation, the Assistant Privacy Commissioner recommended that the organization post the privacy policy on its website, disseminate the privacy policy to its employees and provide staff with proper privacy training. J.J. Barnicke fully implemented the Assistant Commissioner's recommendations.

The complainant filed an application in the Federal Court. A hearing scheduled for November 2007 was adjourned on the basis of a preliminary procedural motion and a new hearing date had not yet been set.

## Monitoring Function

As part of our larger court monitoring function, we continued to monitor several court cases involving novel privacy issues. This is one of the ways in which we stay abreast of possible advancements in the law, whether they be through applications under *PIPEDA*, applications under the *Privacy Act*, the federal *Access to Information Act*, or actions in the provincial superior courts under the common law or Quebec's civil law.

For example, we were granted intervener status in *X. v. The Minister of Health and Privacy Commissioner of Canada*, even though this matter originated under the *Access to Information Act*.

In this case, a journalist sought access to Health Canada's Canadian Adverse Drug Reaction Information System database, which houses mandatory and voluntary reports of adverse reactions to drugs marketed in Canada.

Health Canada refused to reveal the province in which data had been collected on the grounds that this information, together with the already released information, could permit the identification of individuals when combined with publicly available information. The Information Commissioner agreed, holding that the information was exempt from access.

The journalist sought judicial review of Health Canada's decision.

Our Office decided to intervene given the significance of this case in relation to the interpretation and application of both *PIPEDA* and the *Privacy Act*, as well as the

interpretation of the meaning of “personal information.” We argued in favour of a broad definition of personal information.

This case demonstrates the important role we can play as an intervener on issues having a significant impact on *PIPEDA* and/or the *Privacy Act* – and in this way contribute meaningfully towards the development of privacy jurisprudence in Canada.

The Federal Court was to hear the case in February 2008.



## SUBSTANTIALLY SIMILAR PROVINCIAL AND TERRITORIAL LEGISLATION

Section 25(1) of *PIPEDA* requires our Office to report annually to Parliament on the “extent to which the provinces have enacted legislation that is substantially similar” to the Act.

In past annual reports, we have reported on legislation in British Columbia, Alberta, Ontario and Quebec which has been declared substantially similar.

No provinces or territories enacted legislation in 2007 for which they have sought consideration as substantially similar to *PIPEDA*.





# THE YEAR AHEAD

Our key priorities for the coming year:

## **Continue to improve service delivery**

- Design and implement new and innovative investigative strategies to make our complaints resolution process more efficient and effective.

## **Build a sustainable organizational capacity**

- On the human resources side, address retention issues and grow our Office in order to balance workload internally and manage increasing demand for our services.
- Continue an information management renewal project; introduce scanning technology; use current technologies to update inquiry and investigation processes; and modernize our case management system.

## **Support Canadians to make informed privacy decisions**

- Develop materials to help Canadians better understand their privacy rights and take action to protect these rights.
- Prepare and distribute publications and guidelines in print and on the web; continue to reach out using new and interactive technologies such as blogs and online videos.
- Implement a social marketing campaign on children's online privacy.
- Put into place education and outreach programs in partnership with provincial and territorial privacy commissioners.

## **Provide leadership to advance four priority privacy issues**

- Information Technology
  - Build sufficient capacity to assess the privacy impact of new information technologies.
  - Increase public awareness of technologies with potential privacy impacts.
  - Provide practical guidance to organizations on the implementation of specific technologies.

- **National Security**
  - Ensure national security initiatives adequately protect privacy.
  - Ensure proper oversight and accountability of national security agencies' personal information management practices.
  - Raise public awareness of the privacy impacts of national security initiatives.
- **Identity Integrity and Protection / Identity Theft**
  - Improve organizations' personal information management practices.
  - Raise public awareness of identity protection.
  - Persuade the federal government to adopt a coordinated approach to identity protection.
- **Genetic Information**
  - Advance research and knowledge to address new challenges posed by genetics in the context of traditional data protection regimes.
  - Raise public awareness about the potential uses of genetic information.

#### **Advance global privacy protection for Canadians**

- Seek legislative amendments to *PIPEDA*; co-operate with other data protection authorities to ensure privacy protection measures are comprehensive and harmonious.
- Chair an OECD volunteer group reviewing how cooperation between data protection authorities and other privacy rights enforcement agencies can be enhanced.
- Continue to work with an APEC data privacy group which has developed a privacy framework for APEC member states.

## APPENDIX 1 – DEFINITIONS; INVESTIGATION PROCESS

### DEFINITIONS OF COMPLAINT TYPES UNDER *PIPEDA*

---

Complaints received in the OPC are categorized according to the principles and provisions of *PIPEDA* that are alleged to have been contravened:

- **Access.** An individual has been denied access to his or her personal information by an organization, or has not received all the personal information, either because some documents or information are missing or because the organization has applied exemptions to withhold information.
- **Accountability.** An organization has failed to exercise responsibility for personal information in its possession or custody, or has failed to identify an individual responsible for overseeing its compliance with the Act.
- **Accuracy.** An organization has failed to ensure that the personal information it uses is accurate, complete, and up-to-date.
- **Challenging compliance.** An organization has failed to put procedures or policies in place that allow an individual to challenge its compliance with the Act, or has failed to follow its own procedures and policies.
- **Collection.** An organization has collected personal information that is not necessary, or has collected it by unfair or unlawful means.
- **Consent.** An organization has collected, used or disclosed personal information without valid consent, or has made the provision of a good or service conditional on individuals consenting to an unreasonable collection, use, or disclosure.
- **Correction/Notation.** The organization has failed to correct personal information as requested by an individual, or, where it disagrees with the requested correction, has not placed a notation on the information indicating the substance of the disagreement.

- **Fee.** An organization has required more than a minimal fee for providing individuals with access to their personal information.
- **Retention.** Personal information is retained longer than necessary for the fulfillment of the purposes that an organization stated when it collected the information, or, if it has been used to make a decision about an individual, has not been retained long enough to allow the individual access to the information.
- **Safeguards.** An organization has failed to protect personal information with appropriate security safeguards.
- **Time limits.** An organization has failed to provide an individual with access to his or her personal information within the time limits set out in the Act.
- **Use and disclosure.** Personal information is used or disclosed for purposes other than those for which it was collected, without the consent of the individual, and the use or disclosure without consent is not one of the permitted exceptions in the Act.

## DEFINITIONS OF FINDINGS AND OTHER DISPOSITIONS

The Office has developed a series of definitions of findings and dispositions to explain the outcome of its investigations under *PIPEDA*:

- **Not well-founded.** The investigation uncovered no or insufficient evidence to conclude that an organization violated the complainant's rights under *PIPEDA*.
- **Well-founded.** An organization failed to respect a provision of *PIPEDA*.
- **Resolved.** The investigation substantiated the allegations but, prior to the conclusion of the investigation, the organization took or committed to take corrective action to remedy the situation, to the satisfaction of the OPC.
- **Well-founded and resolved.** The Commissioner, being of the view at the conclusion of the investigation that the allegations were likely supported by the evidence, before making a finding made a recommendation to the organization for corrective action to remedy the situation, which the organization took or committed to take.
- **Settled during the course of the investigation.** The OPC helped negotiate a solution that satisfies all involved parties during the course of the investigation. No finding is issued.



- **Discontinued.** The investigation ended before a full investigation of all the allegations. A case may be discontinued for any number of reasons – for instance, the complainant may no longer want to pursue the matter or cannot be located to provide information critical to making a finding.
- **No jurisdiction.** The investigation led to a conclusion that *PIPEDA* did not apply to the organization or activity that was the subject of the complaint.
- **Early resolution.** This applies to situations where the issue was dealt with before a formal investigation occurred. For example, if an individual filed a complaint about a type of issue that the OPC had already investigated and found to comply with *PIPEDA*, we would explain this to the individual. “Early resolution” would also describe the situation where an organization, on learning of allegations against it, addressed them immediately to the satisfaction of the complainant and the OPC.

## INVESTIGATION PROCESS UNDER PIPEDA

### Inquiry:

Individual contacts OPC by letter, by telephone, or in person to complain of violation of Act. Individuals who make contact in person or by telephone must subsequently submit their allegations in writing.



### Initial analysis:

Inquiries staff review the matter to determine whether it constitutes a complaint, i.e., whether the allegations could constitute a contravention of the Act.

An individual may complain about any matter specified in sections 5 to 10 of the Act or in Schedule 1 — for example, denial of access, or unacceptable delay in providing access, to his or her personal information held by an organization; improper collection, use or disclosure of personal information; inaccuracies in personal information used or disclosed by an organization; or inadequate safeguards of an organization's holdings of personal information.



### Complaint?

#### No:

The individual is advised, for example, that the matter is not in our jurisdiction.

#### Yes:

An investigator is assigned to the case.

### Early resolution?

A complaint may be resolved before an investigation is undertaken if, for example, the issue has already been fully dealt with in another complaint and the organization has ceased the practice.

### Investigation:

The investigation provides the factual basis for the Commissioner to determine whether the individual's rights have been contravened under *PIPEDA*.

The investigator writes to the organization, outlining the substance of the complaint. The investigator gathers the facts related to the complaint through representations from both parties and through independent inquiry, interviews of witnesses, and review of documentation. Through the Privacy Commissioner or her delegate, the investigator has the authority to receive evidence, enter premises where appropriate, and examine or obtain copies of records found on any premises.

### Discontinued?

A complaint may be discontinued if, for example, a complainant decides not to pursue it, or a complainant cannot be located.

### Analysis (on next page)

### Settled? (on next page)

**Note:** a broken line (---) indicates a *possible* outcome.

### Analysis:

The investigator analyses the facts and prepares recommendations to the Privacy Commissioner or her delegate. The investigator will contact the parties and review the facts gathered during the course of the investigation. The investigator will also tell the parties what he or she will be recommending, based on the facts, to the Privacy Commissioner or her delegate. At this point, the parties may make further representations.

Analysis will include internal consultations with, for example, Legal Services or Research and Policy Sections, as appropriate.

### Findings:

The Privacy Commissioner or her delegate reviews the file and assesses the report. The Privacy Commissioner or her delegate, not the investigator, decides what the appropriate outcome should be and whether recommendations to the organization are warranted.

### Preliminary report

If the results of the investigation indicate to the Privacy Commissioner or her delegate that there likely has been a contravention of *PIPEDA*, she or her delegate recommends to the organization how to remedy the matter, and asks the organization to indicate within a set time-period how it will implement the recommendation.

### Final Report and Letters of Findings

The Privacy Commissioner or her delegate sends letters of findings to the parties. The letters outline the basis of the complaint, the relevant findings of fact, the analysis, and the response of the organization to any recommendations made in the preliminary report.

The possible findings are:

**Not Well-Founded:** The evidence, on balance, does not lead the Privacy Commissioner or her delegate to conclude that the complainant's rights under the Act have been contravened.

**Well-Founded:** The organization failed to respect a provision of the Act.

**Resolved:** The investigation substantiates the allegations but, prior to the conclusion of the investigation, the organization has taken or has committed to take corrective action to remedy the situation, to the satisfaction of our Office.

**Well-founded and resolved:** The investigation substantiates the allegations but the organization has taken or has committed to take corrective action to remedy the situation, as recommended in the Commissioner's preliminary report at the conclusion of the investigation.

In the letter of findings, the Privacy Commissioner or her delegate informs the complainant of his or her rights of recourse to the Federal Court.

#### Settled?

The OPC seeks to resolve complaints and to prevent contraventions from recurring. The Commissioner encourages resolution through mediation, negotiation and persuasion. The investigator assists in this process.

Where recommendations have been made to an organization, OPC staff will follow up to verify that they have been implemented.

The complainant or the Privacy Commissioner may choose to apply to the Federal Court for a hearing of the matter. The Federal Court has the power to order the organization to correct its practices and to publish a notice of any action taken or proposed to correct its practices. The Court can award damages to a complainant, including damages for humiliation. There is no ceiling on the amount of damages.

**Note:** a broken line (---) indicates a *possible* outcome.



# APPENDIX 2 – INQUIRY AND INVESTIGATION STATISTICS

## Inquiries Statistics

Our Inquiries Unit provides one of our most important services to Canadians – quick, direct and personalized information about privacy issues. We received almost 8,000 *PIPEDA*-related inquiries in 2007.

Frequently raised issues include: the collection and use of Social Insurance Numbers; obtaining access to personal data held by financial institutions; and use and disclosure of personal information in the telecommunications and sales sectors. Identity theft is another key issue people contact us about. Police often advise individuals who have filed police reports about identity theft to get in touch with our Office for further information.

We have recently seen heightened interest by organizations about transborder issues.

For the period between January 1 and December 31, 2007

PIPEDA inquiries received by the Inquiries Unit	
Telephone inquiries	6,428
Written inquiries (letter and fax)	1,208
Total number of inquiries received	7,636
PIPEDA inquiries closed by the Inquiries Unit	
Telephone inquiries	6,417
Written inquiries (letter and fax)	1,142
Total number of inquiries closed	7,559



## COMPLAINTS RECEIVED BY TYPE

By far, the largest number of complaints we receive involve how organizations have used and disclosed information. The most common type of use and disclosure complaint involves an allegation of personal information being used for purposes other than for which it was collected, and being disclosed to third parties without an individual's consent.

Collection complaints usually concern the collection of information without proper consent or the collection of more information than required for the stated purpose.

Access complaints deal mainly with allegations that organizations have not responded to requests for personal information or have not provided all of the information to which individuals believe they are entitled.

### Complaints received between January 1, 2007 and December 31, 2007

Complaint type	Count	Percentage
Use and Disclosure	120	34
Collection	68	19
Access	67	19
Safeguards	36	10
Consent	16	5
Time Limits	13	4
Accountability	8	2
Accuracy	7	2
Retention	7	2
Openness	4	1
Correction/Notation	3	1
Fee	1	<1
<b>Total</b>	<b>350</b>	

**BREAKDOWN BY SECTOR**

Complaints received between January 1 and December 31, 2007

Sector	Count	Percentage
Financial Institutions	105	30
Telecommunications	42	12
Other	39	11
Sales	37	11
Insurance	35	10
Transportation	28	8
Professionals	26	7
Accommodation	21	6
Health	9	2.5
Services	6	2
Rental	2	<1
<b>Total</b>	<b>350</b>	

**CATEGORIES**

**Financial Institutions:** Banks, collection agencies, credit bureaus, credit grantors, financial advisors

**Telecommunications:** Broadcasters, cable/satellite, telephone, telephone/wireless, Internet services

**Other:** For example, private schools, aboriginal bands, security companies and private investigators.

**Sales:** Car dealerships, pharmacies, real estate, retail, stores

**Insurance:** Life and health insurance, property and casualty insurance

**Transportation:** Air, land, rail, water

**Professionals:** Accountants, lawyers

**Accommodation:** Hotels, landlords, condominiums, property management

**Health:** Chiropractors, dentists, doctors, physiotherapists, psychologists/psychiatrists

**Services:** Daycare, hairdressers, beauticians

**Rental:** Car rental, other rental

**CLOSED COMPLAINTS BY COMPLAINT TYPE**

Complaints closed between January 1, 2007 and December 31, 2007

Complaint type	Count	Percentage
Use and Disclosure	162	39
Collection	80	19
Access	68	16
Safeguards	37	9
Consent	25	6
Time Limits	11	3
Accountability	9	2
Retention	9	2
Correction/Notation	7	2
Accuracy	5	1
Openness	4	1
Other (Retaliation)*	2	<1
Fee	1	<1
<b>Total</b>	<b>420</b>	

\* We closed two retaliation or “whistle-blowing” complaints. The enforcement of retaliation complaints is included under section 27.1 of *PIPEDA*. The provision is aimed at ensuring that organizations do not retaliate against employees who have, in good faith, brought forward allegations that their employers have contravened *PIPEDA* or will contravene *PIPEDA*, or that an employee has refused to do something that would contravene the legislation. Retaliation could include, for example, dismissal, suspension, demotion, or discipline.

The Commissioner, in her ombudsman role, has an obligation to investigate retaliation cases to determine whether she should forward them to the Attorney General of Canada for possible prosecution under the Criminal Code. While our Office has assessed retaliation complaints, no cases have warranted follow-up with the Attorney General.

Number of complaints in abeyance

(awaiting assignment to an investigator) on December 31, 2007: 44

## CLOSED COMPLAINTS BY FINDING

Almost one third of our closed complaints were settled. This indicates that, in a large number of cases, we were successful in finding solutions that satisfied complainants, respondents and this Office.

The next-largest category was discontinued. Cases are discontinued for a number of reasons – complainants abandon complaints for personal reasons or because an organization resolves an issue before the investigation has begun or our Office can't proceed because a complainant hasn't provided us with requested additional details necessary to complete an investigation.

### Complaints closed between January 1, 2007 and December 31, 2007

Finding	Count	Percentage
Settled	125	30
Discontinued	89	21
Not well-founded	64	15
Well-founded Resolved	62	15
Resolved	41	10
Early Resolution	14	3
No jurisdiction	14	3
Well-founded	9	2
Other (Retaliation)	2	<1
<b>TOTAL</b>	<b>420</b>	

**PIPEDA INVESTIGATION TREATMENT TIMES - BY FINDING**

Roughly one-quarter of our investigations are completed within a year. More complex cases take longer to complete. For example, cases involving multi-jurisdictional issues or which require extensive research into industry practices usually take more time to complete. In some instances, cases take longer if there are delays in obtaining information.

For the period between January 1 and December 31, 2007

Disposition	Average Treatment Time in Months
Early Resolution	3.36
Discontinued	11.18
No jurisdiction	12.07
Settled	12.17
Not well-founded	20.56
Resolved	20.68
Well-founded Resolved	23.15
Well-founded	24.36
Other (Retaliation)	26.00
<b>Overall Average</b>	<b>15.71</b>



**FINDINGS BY COMPLAINT TYPE**

Complaints closed between January 1, 2007 and December 31, 2007

	Discontinued	Early Resolution	No Jurisdiction	Not Well founded	Other	Resolved	Settled	Well-founded	Well founded Resolved	TOTAL
Use and Disclosure	26	8	6	27	0	8	46	3	38	162
Collection	18	2	2	18	0	7	25	2	6	80
Access	17	2	5	4	0	15	19	1	5	68
Safeguards	9	1	0	4	0	3	11	1	8	37
Consent	7	1	1	2	0	5	7	0	2	25
Time Limits	4	0	0	0	0	2	3	2	0	11
Accountability	0	0	0	2	0	1	5	0	1	9
Retention	2	0	0	2	0	0	5	0	0	9
Correction/Notation	3	0	0	3	0	0	0	0	1	7
Accuracy	2	0	0	1	0	0	1	0	1	5
Openness	0	0	0	1	0	0	3	0	0	4
Other	0	0	0	0	2	0	0	0	0	2
Fee	1	0	0	0	0	0	0	0	0	1
<b>TOTAL</b>	<b>89</b>	<b>14</b>	<b>14</b>	<b>64</b>	<b>2</b>	<b>41</b>	<b>125</b>	<b>9</b>	<b>62</b>	<b>420</b>

**FINDINGS BY INDUSTRY SECTOR**

Complaints closed between January 1, 2007 and December 31, 2007

	Discontinued	Early Resolution	No Jurisdiction	Not Well-founded	Other	Resolved	Settled	Well-founded	Well-founded Resolved	TOTAL
Financial Institutions	24	5	3	21	0	14	28	0	18	113
Telecommunications	11	2	2	12	1	5	17	4	17	71
Sales	7	3	1	2	0	5	34	0	9	61
Other	17	0	7	8	0	2	23	0	1	58
Insurance	13	2	0	3	0	6	11	1	8	44
Transportation	4	1	0	11	1	4	7	2	3	33
Professionals	3	1	1	2	0	2	1	2	2	14
Services	2	0	0	4	0	1	0	0	4	11
Accommodations	7	0	0	0	0	0	2	0	0	9
Rental	0	0	0	0	0	2	2	0	0	4
Health	1	0	0	1	0	0	0	0	0	2
<b>TOTAL</b>	<b>89</b>	<b>14</b>	<b>14</b>	<b>64</b>	<b>2</b>	<b>41</b>	<b>125</b>	<b>9</b>	<b>62</b>	<b>420</b>

**PIPEDA INVESTIGATION TREATMENT TIMES - BY COMPLAINT TYPE**

For the period between January 1 and December 31, 2007

Complaint Type	Average Treatment Time in Months
Accuracy	9.4*
Fee	10.0*
Time Limits	11.3
Retention	12.7
Access	14.5
Openness	15.3*
Correction/Notation	15.4
Use and Disclosure	15.8
Safeguards	15.9
Accountability	16.2
Collection	17.0
Consent	18.0
Other	26.0*
<b>Overall average</b>	15.7

\*The treatment time for these complaint types reflects 6 or fewer cases each.







# **DÉLAIS DE TRAITEMENT DES ENQUÊTES EN VERTU DE LA LRPDÉ — PAR TYPE DE PLAINTÉ**

Période allant du 1<sup>er</sup> janvier au 31 décembre 2007

Type de plainte	Délai moyen de traitement en mois
Exactitude	9,4*
Frais	10,0*
Délais	11,3
Conservation	12,7
Accès	14,5
Transparence	15,3*
Correction/Annotation	15,4
Utilisation et communication	15,8
Mesures de sécurité	15,9
Responsabilité	16,2
Collecte	17,0
Consentement	18,0
Autres	26,0*
Moyenne globale	15,7

\* Le délai de traitement pour ces types de plaintes se rapporte chaque fois à six cas ou moins.

CONCLUSIONS PAR SECTEUR INDUSTRIEL

Plaintes résolues entre le 1<sup>er</sup> janvier et le 31 décembre 2007

	Reglée rapide	Hors jurisdiction	Non fondee	Autres	Resolue	Reglee	Fondee	Fondee et resolue	TOTAL
--	------------------	----------------------	---------------	--------	---------	--------	--------	-------------------------	-------

Institutions financieres	24	5	3	21	0	14	28	0	18	113
Telecom- munications	11	2	2	12	1	5	17	4	17	71
Ventes	7	3	1	2	0	5	34	0	9	61
Autres	17	0	7	8	0	2	23	0	1	58
Assurance	13	2	0	3	0	6	11	1	8	44
Transport	4	1	0	11	1	4	7	2	3	33
Services professionnels	3	1	1	2	0	2	1	2	2	14
Services	2	0	0	4	0	1	0	0	4	11
Hebergement	7	0	0	0	0	0	2	0	0	9
Location	0	0	0	0	0	2	2	0	0	4
Sante	1	0	0	1	0	0	0	0	0	2
TOTAL	89	14	14	64	2	41	125	9	62	420

## CONCLUSIONS PAR TYPE DE PLAINTÉ

Plaintes résolues entre le 1<sup>er</sup> janvier et le 31 décembre 2007

	Abandonnée	Réglement rapide	Hors juridiction	Non fondée	Autres	Réglée	Fondée	Fondée et résolue	TOTAL
--	------------	---------------------	---------------------	---------------	--------	--------	--------	-------------------------	-------

Utilisation et communication	26	8	6	27	0	8	46	3	38	162
Collecte	18	2	2	18	0	7	25	2	6	80
Accès	17	2	5	4	0	15	19	1	5	68
Mesures de sécurité	9	1	0	4	0	3	11	1	8	37
Consentement	7	1	1	2	0	5	7	0	2	25
Délais	4	0	0	0	0	2	3	2	0	11
Responsabilité	0	0	0	2	0	1	5	0	1	9
Conservation	2	0	0	2	0	0	5	0	0	9
Correction/Annotation	3	0	0	3	0	0	0	0	1	7
Exactitude	2	0	0	1	0	0	1	0	1	5
Transparence	0	0	0	1	0	0	3	0	0	4
Autres	0	0	0	0	2	0	0	0	0	2
Frais	1	0	0	0	0	0	0	0	0	1
<b>TOTAL</b>	<b>89</b>	<b>14</b>	<b>14</b>	<b>64</b>	<b>2</b>	<b>41</b>	<b>125</b>	<b>9</b>	<b>62</b>	<b>420</b>

DÉLAIS DE TRAITEMENT DES ENQUÊTES EN VERTU DE LA LPPDÉ — PAR TYPE DE CONCLUSION

Environ le quart de nos enquêtes sont menées à terme en moins d'un an. Les cas plus complexes demandent davantage de temps. À titre d'exemple, les cas impliquant plusieurs administrations ou nécessitant une recherche exhaustive dans les pratiques industrielles seront habituellement plus longs à régler. Parfois, les cas s'étirent parce que l'information se fait attendre.

Période allant du 1<sup>er</sup> janvier au 31 décembre 2007

Décision		Délai moyen de traitement en mois
Réglée rapidement		3,36
Abandonnée		11,18
Hors juridiction		12,07
Réglée en cours d'enquête		12,17
Non fondée		20,56
Résolue		20,68
Fondée et résolue		23,15
Fondée		24,36
Autres (représailles)		26,00
Moyenne globale		15,71

PLAINTES RÉSOLUES PAR TYPE DE CONCLUSION

Près du tiers de nos plaintes résolues ont été réglées. En d'autres mots, nous avons réussi dans un grand nombre de cas à trouver des solutions qui ont satisfait les plaignants, les parties intimées et le Commissariat.

La deuxième plus grande catégorie est celle des cas abandonnés. Plusieurs raisons peuvent expliquer une telle situation, comme des motifs personnels, parce qu'une organisation a réglé une question avant le début de l'enquête, ou parce que le Commissariat ne peut aller de l'avant étant donné qu'un plaignant ne lui a pas fourni les détails additionnels nécessaires pour réaliser une enquête.

Plaintes résolues entre le 1<sup>er</sup> janvier et le 31 décembre 2007

Conclusions	Nombre	Pourcentage
Réglée en cours d'enquête	125	30
Abandonnée	89	21
Non fondée	64	15
Fondée et résolue	62	15
Réglée	41	10
Réglée rapidement	14	3
Hors juridiction	14	3
Fondée	9	2
Autres (représailles)	2	< 1
<b>TOTAL</b>	<b>420</b>	



PLAINTES RÉSOLUES PAR TYPE DE PLAINTÉ

Plaintes résolues entre le 1<sup>er</sup> janvier et le 31 décembre 2007

Type de plainte	Nombre	Pourcentage
Utilisation et communication	162	39
Collecte	80	19
Accès	68	16
Mesures de sécurité	37	9
Consentement	25	6
Délais	11	3
Responsabilité	9	2
Conservation	9	2
Correction/Annotation	7	2
Exactitude	5	1
Transparence	4	1
Autres (représailles)*	2	<1
Frais	1	<1
Total	420	

\* Nous avons résolu deux plaintes liées à des représailles ou à une dénonciation. L'exécution des mesures entourant les plaintes liées à des représailles est visée par l'article 27.1 de la *LRPDE*. La disposition a pour objet de s'assurer que les organisations ne prennent pas de représailles contre les employés qui ont allégué, de bonne foi, que leur employeur avait enfreint la *LRPDE* ou allait enfreindre la *LRPDE* ou qui ont refusé de faire quelque chose qui aurait été à l'encontre de la Loi. Les représailles peuvent inclure, entre autres, le renvoi, la suspension, la rétrogradation et les mesures disciplinaires.

La commissaire, dans son rôle d'ombudsman, est tenue de faire enquête sur les cas de représailles afin de déterminer si elle doit les signaler au procureur général du Canada en vue d'une éventuelle poursuite judiciaire aux termes du *Code criminel*. Le Commissariat a évalué des plaintes liées à des représailles, mais aucun cas n'a mérité d'être confié au procureur général.

Nombre de plaintes en attente

(en attente d'une attribution à un enquêteur) au 31 décembre 2007 : 44

RÉPARTITION PAR SECTEUR

Plaintes reçues entre le 1<sup>er</sup> janvier et le 31 décembre 2007

Secteur	Nombre	Pourcentage
Institutions financières	105	30
Télécommunications	42	12
Autres	39	11
Ventes	37	11
Assurance	35	10
Transport	28	8
Services professionnels	26	7
Hébergement	21	6
Santé	9	2,5
Services	6	2
Location	2	<1
Total	350	

CATÉGORIES

**Institutions financières** : banques, agences de recouvrement, agences d'évaluation du crédit, fournisseurs de crédit, conseillers financiers

**Télécommunications** : diffuseurs, câble/satellite, téléphone, téléphone sans fil, services Internet

**Autres** : écoles privées, bandes autochtones, compagnies de sécurité, enquêteurs privés, etc.

**Ventes** : concessionnaires d'automobiles, pharmacies, immobilier, vente au détail, magasins

**Assurance** : assurance-vie et assurance-santé, assurance sur les biens et assurance risques divers

**Transport** : aérien, terrestre, ferroviaire, maritime

**Services professionnels** : comptables, avocats

**Hébergement** : hôtels, locations, condominiums, gestion des biens

**Santé** : chiropraticiens, dentistes, médecins, physiothérapeutes, psychologues/psychiatres

**Services** : garderie, coiffeuses, esthéticiennes

**Location** : location d'autos et autres

PLAINTES REÇUES PAR TYPE DE PLAINTE

Les plaintes reçues en plus grand nombre sont de loin celles qui concernent la façon dont les organisations utilisent et communiquent les renseignements. Les plaignants allèguent le plus souvent que les renseignements sont utilisés et communiqués à des fins autres que celles pour lesquelles on les a recueillis, et qu'ils sont communiqués à des tiers sans le consentement du principal intéressé.

Les plaintes relatives à la collecte concernent habituellement la collecte de renseignements sans le consentement approprié ou la collecte de renseignements non requis pour les fins convenues.

Les plaintes relatives à l'accès concernent essentiellement les allégations selon lesquelles les organisations n'ont pas répondu aux demandes de renseignements personnels ou n'ont pas fourni tous les renseignements auxquels les intéressés croient avoir droit.

Plaintes reçues entre le 1<sup>er</sup> janvier et le 31 décembre 2007

Type de plainte	Nombre	Pourcentage
Utilisation et communication	120	34
Collecte	68	19
Accès	67	19
Mesures de sécurité	36	10
Consentement	16	5
Délais	13	4
Responsabilité	8	2
Exactitude	7	2
Conservation	7	2
Transparence	4	1
Correction/Annotation	3	1
Frais	1	<1
Total	350	

# ANNEXE 2 – STATISTIQUES EN MATIÈRE D'ENQUÊTES ET DE DEMANDES DE RENSEIGNEMENTS

## Statistiques sur les demandes de renseignements

Notre Section des demandes de renseignements fournit l'un de nos plus importants services aux Canadiennes et Canadiens – la prestation rapide, directe et personnalisée de renseignements sur les enjeux relatifs à la protection de la vie privée. Nous avons reçu près de 8 000 demandes de renseignements liées à la *LPRPDE* en 2007.

Au nombre des questions fréquemment soulevées, mentionnons les suivantes : la collecte et l'utilisation des numéros d'assurance sociale; l'accès aux données personnelles détenues par les institutions financières; l'utilisation et la communication de renseignements personnels dans les secteurs des télécommunications et des ventes. Le vol d'identité constitue une autre raison importante pour laquelle les gens communiquent avec nous. Les forces policières conseillent souvent aux personnes qui ont rempli un rapport de police sur un vol d'identité de communiquer avec le Commissariat pour obtenir de plus amples détails.

Nous avons récemment constaté un intérêt accru des organisations à l'égard des questions transfrontalières.

Période allant du 1<sup>er</sup> janvier au 31 décembre 2007

Demandes de renseignements en vertu de la <i>LPRPDE</i> reçues par la Section des demandes de renseignements		
Demandes de renseignements téléphoniques	6 428	
Demandes de renseignements écrites (lettre et télécopie)	1 208	
Nombre total de demandes reçues	7 636	

Demandes de renseignements en vertu de la <i>LPRPDE</i> réglées par la Section des demandes de renseignements		
Demandes de renseignements téléphoniques	6 417	
Demandes de renseignements écrites (lettre et télécopie)	1 142	
Nombre total de demandes résolues	7 559	





L'enquêteur analyse les faits et formule ses recommandations à l'intention de la commissaire à la protection de la vie privée ou de sa déléguée. Il informe également les parties des recommandations fondées sur l'analyse des faits qu'il remettra à la commissaire ou à sa déléguée. À cette étape, les parties peuvent faire d'autres auditions d'arguments.

Au besoin, des consultations internes sont effectuées avec, par exemple, le concours de la Section des services juridiques ou de la Section de la recherche et des politiques.

## Analyse

## Conclusions

La commissaire à la protection de la vie privée ou sa déléguée examine le dossier et évalue le rapport. La commissaire ou sa déléguée, et non l'enquêteur, détermine les conclusions à tirer et décide s'il faut présenter des recommandations à l'organisation.

## Rapport préliminaire

Si les résultats de l'enquête permettent de conclure qu'il y avait selon toute probabilité infraction à la *Loi sur l'accès à l'information*, la commissaire à la protection de la vie privée ou sa déléguée recommande à l'organisation des mesures pour remédier au problème et lui demande de lui indiquer dans un délai précis comment elle entend mettre ces mesures en œuvre.

## Rapport final et lettre de conclusions

La commissaire ou sa déléguée envoie la lettre de conclusions d'enquêtes aux parties. Cette lettre présente la plainte, les faits établis, l'analyse et la réponse de l'organisation à toute recommandation faite dans le cadre du rapport préliminaire.

Les conclusions possibles sont les suivantes :

**Non fondée** : La preuve ne permet pas à la commissaire à la protection de la vie privée ou à sa déléguée de conclure que le droit à la protection de la vie privée de l'organisation a été enfreint.

**Fondée** : L'organisation n'a pas respecté l'une des dispositions de la Loi.

**Résolue** : La preuve recueillie au cours de l'enquête donne raison au plaignant mais, avant que l'enquête ne soit terminée, l'organisation a pris ou s'est engagée à prendre des mesures pour corriger le problème.

**Fondée et résolue** : L'enquête donne raison au plaignant, et l'organisation a pris ou s'est engagée à prendre les mesures correctives recommandées dans le rapport préliminaire de la commissaire, au terme de l'enquête.

Dans la lettre de conclusions, la commissaire à la protection de la vie privée ou sa déléguée informe le plaignant de son droit de recours devant la Cour fédérale.

## Plainte résolue?

Le CPVP cherche à résoudre les plaintes et à prévenir d'autres infractions à la Loi. La commissaire favorise la résolution des différends par l'entremise de la médiation, de la négociation et de la persuasion. L'enquêteur participe au processus.

Lorsque des recommandations sont présentées à une organisation, des employés du CPVP effectuent un suivi pour vérifier si elles ont bel et bien été appliquées.

Le plaignant ou la commissaire à la protection de la vie privée peut choisir de demander une audience devant la Cour fédérale. La Cour fédérale a le pouvoir d'ordonner à une organisation de corriger ses pratiques ainsi que de publier un avis énonçant les mesures prises ou envisagées pour corriger ses pratiques. La Cour peut accorder des dommages et intérêts au plaignant, notamment en réparation de l'humiliation subie. Il n'existe pas de plafond pour ces dommages-intérêts.

Note : une ligne discontinue (---) indique un résultat possible.

## PROCESSUS D'ENQUÊTE EN VERTU DE LA LRPDÉ

### Demande de renseignements

Une personne qui croit que la Loi a été enfreinte communique avec le CVP par téléphone, par lettre ou en personne. Si la personne décide de communiquer avec le CVP par téléphone ou en personne, elle devra ensuite présenter ses allégations par écrit.

### Analyse initiale

Le personnel des demandes de renseignements examine le dossier afin d'établir s'il s'agit d'une plainte, c'est-à-dire si la loi a possiblement été enfreinte.

Une personne peut déposer une plainte aux termes des articles 5 à 10 ou de l'Annexe I de la Loi. Par exemple, une plainte peut porter sur : 1) le refus, par une organisation, de fournir à une personne ses renseignements personnels ou de les lui fournir dans les délais prescrits par la Loi; 2) la collecte, l'utilisation ou la communication inappropriée de renseignements personnels; 3) l'utilisation ou la communication de renseignements inexacts au sujet d'une personne; 4) l'absence de mesures de sécurité pour assurer la protection des renseignements personnels détenus par une organisation, etc.

### Plainte?

#### Refusée

La personne est avisée, par exemple, que la demande ne relève pas de notre juridiction.

#### Acceptée

Un enquêteur est chargé de l'affaire.

### Enquête

L'enquête permet d'établir les faits; la commissaire détermine ensuite si le droit à la protection de la vie privée du plaignant en vertu de la LRPDÉ a été enfreint.

L'enquêteur écrit à l'organisation pour lui présenter l'objet de la plainte. Il établit les faits grâce à l'audition d'arguments des deux parties, à la tenue d'une enquête indépendante, à l'interrogation des témoins et à l'examen de la documentation. L'enquêteur peut, de par les pouvoirs conférés par la commissaire ou par sa déléguée, recevoir des éléments de preuve, visiter les locaux de l'organisation au besoin et examiner ou se faire remettre des copies de documents trouvés dans les locaux visités.

### Règlement rapide?

Une plainte peut être résolue avant le début de l'enquête; par exemple, le problème peut avoir fait l'objet d'une plainte antérieure et, depuis, l'organisation concernée a mis fin à la pratique problématique.

### Plainte abandonnée?

Il est possible qu'une plainte soit abandonnée dans des cas où, par exemple, la personne qui s'est plainte décide d'abandonner l'affaire ou est impossible à trouver.

### Plainte résolue? (suite)

### Analyse (suite)

Note : une ligne discontinue (---) indique un résultat possible.

- **Réglée en cours d'enquête.** Le CPVP aide à négocier, en cours d'enquête, une solution qui convient à toutes les parties. Aucune conclusion n'est rendue.
- **Abandonnée.** Il s'agit d'une enquête qui est terminée avant que toutes les allégations ne soient pleinement examinées. Une affaire peut être abandonnée pour toutes sortes de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire ou il est impossible de lui demander de fournir des renseignements supplémentaires, lesquels sont essentiels pour en arriver à une conclusion.
- **Hors juridiction.** L'enquête a démontré que la *LRPDE* ne s'applique pas à l'organisation ou à l'activité faisant l'objet de la plainte.
- **Réglée rapidement.** Situation dans laquelle l'affaire est réglée avant même qu'une enquête officielle ne soit entreprise. À titre d'exemple, si une personne dépose une plainte concernant un sujet qui a déjà fait l'objet d'une enquête par le CPVP et qui a été jugé conforme à la *LRPDE*, nous donnons les explications nécessaires à la personne plaignante. Cette conclusion s'applique également lorsqu'une organisation, mise au courant des allégations, règle immédiatement la question à la satisfaction du plaignant et du CPVP.

de désaccord avec les corrections demandées, n'a pas annoté les renseignements afin d'indiquer la teneur du désaccord.

- **Frais.** Une organisation a exigé plus que des frais minimaux pour fournir à des personnes l'accès à leurs renseignements personnels.
- **Conservation.** Les renseignements personnels sont conservés plus longtemps qu'il n'est nécessaire aux fins qu'une organisation a déclarées au moment de la collecte des renseignements ou, s'ils ont été utilisés pour prendre une décision au sujet d'une personne, l'organisation n'a pas conservé les renseignements assez longtemps pour permettre à la personne d'y avoir accès.
- **Mesures de sécurité.** Une organisation n'a pas protégé les renseignements personnels qu'elle détient par des mesures de sécurité appropriées.
- **Délais.** Une organisation a omis de fournir à une personne l'accès aux renseignements personnels qui la concernent dans les délais prévus par la Loi.
- **Utilisation et communication.** Les renseignements personnels sont utilisés ou communiqués à des fins autres que celles pour lesquelles ils avaient été recueillis, sans le consentement de la personne concernée, et l'utilisation ou la communication de renseignements personnels sans le consentement de la personne concernée ne font pas partie des exceptions prévues dans la Loi.

## DEFINITIONS DES CONCLUSIONS ET D'AUTRES DISPOSITIONS

Le CPVP a élaboré des définitions de conclusions et de décisions afin d'expliquer les résultats des enquêtes effectuées conformément à la *LRPPE* :

- **Non fondée.** L'enquête n'a pas permis de déceler des éléments de preuves qui suffisent à conclure qu'une organisation a enfreint les droits du plaignant en vertu de la *LRPPE*.

- **Fondée.** L'organisation n'a pas respecté une disposition de la *LRPPE*.

- **Résolue.** L'enquête a corroboré les allégations, mais avant la fin de l'enquête, l'organisation a pris des mesures correctives pour remédier à la situation, à la satisfaction du CPVP, ou s'est engagée à prendre ces mesures.

- **Fondée et résolue.** La commissaire est d'avis, au terme de son enquête, que les allégations semblent fondées sur des preuves, mais fait une recommandation à l'organisation concernée avant de rendre ses conclusions, et l'organisation prend ou s'engage à prendre les mesures correctives recommandées.

## DÉFINITIONS DES TYPES DE PLAINTES DÉPOSÉES EN VERTU DE LA LRPDÉ

Les plaintes adressées au CPVP sont réparties selon les principes et les dispositions de la LRPDÉ qui auraient été enfreints :

- **Accès.** Une personne s'est vue refuser l'accès aux renseignements personnels qu'une organisation détient à son sujet ou n'a pas reçu tous les renseignements, soit en raison de l'absence de certains documents ou renseignements ou parce que l'organisation a invoqué des exceptions afin de soustraire les renseignements.

- **Responsabilité.** Une organisation a failli à l'exercice de ses responsabilités à l'égard des renseignements personnels qu'elle possède ou qu'elle garde ou elle a omis de désigner une personne responsable de surveiller l'application de la Loi.
- **Exactitude.** Une organisation a omis de s'assurer que les renseignements personnels qu'elle utilise sont exacts, complets et à jour.

- **Possibilité de porter plainte.** Une organisation a omis de mettre en place les procédures ou les politiques qui permettent à une personne de porter plainte en vertu de la Loi ou elle a enfreint ses propres procédures et politiques.
- **Collecte.** Une organisation a recueilli des renseignements personnels non nécessaires ou les a recueillis par des moyens injustes ou illégaux.

- **Consentement.** Une organisation a recueilli, utilisé ou communiqué des renseignements personnels sans le consentement de la personne concernée ou elle a fourni des biens et des services à la condition que la personne consente à la collecte, à l'utilisation ou à la communication déraisonnable de renseignements personnels.

- **Correction/Annotation.** L'organisation n'a pas corrigé, à la demande d'une personne, les renseignements personnels qu'elle détient à son sujet ou, en cas



- Développer suffisamment de capacités pour évaluer les répercussions des nouvelles technologies de l'information sur la protection de la vie privée.
- Sensibiliser davantage le public aux technologies ayant une incidence sur la vie privée.
- Fournir une orientation pratique aux organisations sur la mise en œuvre de technologies particulières.

- Sécurité nationale

- Veiller à ce que les initiatives axées sur la sécurité nationale protègent adéquatement la vie privée.
- Surveiller adéquatement, chez les organismes chargés de la sécurité nationale, les pratiques de gestion des renseignements personnels et voir à ce que ces organismes se responsabilisent.
- Sensibiliser le public aux incidences pour la vie privée des initiatives en matière de sécurité nationale.

- Intégrité et protection de l'identité, vol d'identité

- Améliorer les pratiques de gestion des renseignements personnels des organisations.
- Sensibiliser le public à la protection de l'identité.
- Persuader le gouvernement fédéral d'adopter une approche coordonnée en matière de protection de l'identité.

- Information génétique

- Promouvoir la recherche et les connaissances pour relever les nouveaux défis posés par la génétique dans le contexte des régimes conventionnels de protection des données.
- Sensibiliser le public aux utilisations possibles de l'information génétique.

## Promouvoir la protection mondiale de la vie privée pour les Canadiennes et

### Canadiens

- Chercher à apporter des modifications à la *LPDP*; coopérer avec d'autres

autorités de protection des données pour s'assurer que les mesures prises pour

protéger la vie privée sont complètes et harmonieuses.

- Présider un groupe de bénévoles de l'OCCDF chargé d'examiner des moyens

d'améliorer la coopération entre les autorités de protection des données et

d'autres organes d'application du droit à la vie privée.

- Continuer de travailler avec un groupe de l'APFC axé sur la confidentialité des

données qui a élaboré un cadre de protection de la vie privée à l'intention de ses

pays membres.

Nos priorités clés pour l'année à venir sont les suivantes :

## Continuer à améliorer la prestation des services

- Concevoir et mettre en œuvre des stratégies d'enquête nouvelles et novatrices pour améliorer l'efficacité de notre processus de résolution des plaintes.

## Développer des capacités organisationnelles durables

- Sur le plan des ressources humaines, se pencher sur la question du maintien en place de l'effectif et élargir le Commissariat afin d'équilibrer la charge de travail à l'interne et de gérer la demande croissante pour ce qui est de nos services.
- Poursuivre un projet de renouvellement de la gestion de l'information; adopter la technologie du balayage; utiliser les technologies actuelles pour mettre à jour les processus d'enquête et de demandes de renseignements; moderniser notre système de gestion des cas.

## Aider les Canadiennes et Canadiens à prendre des décisions éclairées en matière de protection de la vie privée

- Elaborer du matériel pour aider les Canadiennes et Canadiens à mieux comprendre leur droit à la protection de la vie privée et à prendre des mesures pour protéger ce droit.
- Préparer et distribuer des publications et des lignes directrices sur supports imprimé et électronique; continuer d'entrer en contact avec les gens au moyen de technologies nouvelles et interactives telles que des blogues et des vidéos en ligne.
- Mettre en œuvre une campagne de marketing social sur la protection de la vie privée des enfants en ligne.
- Mettre en place des programmes de sensibilisation et d'éducation en partenariat avec les commissaires à la protection de la vie privée des provinces et des territoires.

## Exercer du leadership pour promouvoir quatre questions prioritaires en matière de protection de la vie privée

- Technologie de l'information



## LOIS PROVINCIALES ET TERRITORIALES ESSENTIELLEMENT SIMILAIRES

Selon le paragraphe 25(1) de la *LPRPDE*, le Commissariat est tenu de déposer annuellement devant le Parlement un rapport sur « la mesure dans laquelle les provinces ont édicté des lois essentiellement similaires » à la Loi.

Dans les rapports annuels passés, nous avons fait rapport sur la législation en Colombie-Britannique, en Alberta, en Ontario et au Québec, qui a été déclarée essentiellement similaire.

Aucune province ni aucun territoire n'a adopté en 2007 de loi pour laquelle on a demandé le statut de loi essentiellement similaire à la *LPRPDE*.





*la protection des renseignements personnels*, de la *Loi sur l'accès à l'information* à l'échelon fédéral ou même de poursuites entendues par des tribunaux provinciaux de haute instance au titre de la common law ou du droit civil du Québec.

À titre d'exemple, on nous a accordé le statut d'intervenant dans l'affaire *X. c. le ministre de la Santé et la commissionaire à la protection de la vie privée du Canada*, même si l'affaire découlait d'abord de la *Loi sur l'accès à l'information*.

Dans cette affaire, un journaliste cherchait à accéder à la base de données du système canadien d'information sur les effets indésirables des médicaments de Santé Canada, qui contient des déclarations obligatoires et volontaires sur les effets indésirables des médicaments mis en vente au Canada.

Santé Canada a refusé de révéler la province dans laquelle les données avaient été recueillies en invoquant le fait que cette information, en plus de l'information déjà diffusée, pourrait permettre d'identifier des personnes si on les combinait à des renseignements publiquement accessibles. Le commissaire à l'information était d'accord, faisant valoir que les renseignements étaient soustraits à l'application de la loi sur l'accès. Le journaliste a demandé à ce que la décision de Santé Canada fasse l'objet d'un contrôle judiciaire.

Le Commissariat a décidé d'intervenir compte tenu de l'importance de l'affaire pour l'interprétation et l'application de la *LRPDE* et de la *Loi sur la protection des renseignements personnels*, ainsi que pour l'interprétation du sens de l'expression « renseignements personnels ». Nous avons plaidé en faveur d'une définition étendue.

Cette affaire démontre le rôle important que nous pouvons jouer comme intervenant sur des questions ayant de profondes répercussions sur la *LRPDE* et/ou sur la *Loi sur la protection des renseignements personnels* – contribuant ainsi de façon valable à l'évolution de la jurisprudence en matière de protection de la vie privée au Canada.

La Cour fédérale devait entendre l'affaire en février 2008.

La commissaire adjointe a conclu que l'organisation avait par ailleurs raison de retenir des renseignements qui contenaient des renseignements personnels d'autres personnes ou étaient protégés par le secret professionnel.

Le plaignant a fait une demande d'audience auprès de la Cour fédérale en vertu de l'article 14 de la *LPRPDE*. La demande a été rejetée par la suite.

*X. c. J.J. Barnicke Ltd.*

N° de dossier de la Cour fédérale : T-1349-06

Une personne a porté plainte contre J.J. Barnicke Ltd. en prétendant que la société recueillait des renseignements personnels de façon inappropriée et appliquait des politiques inadéquates pour les protéger. Le vice-président de la compagnie avait expédié un courriel à tous les employés demandant si quelqu'un connaissait l'entreprise pour laquelle travaillait le plaignant.

Selon la commissaire adjointe à la protection de la vie privée, comme il n'y avait aucune preuve qu'un employé de J.J. Barnicke avait répondu au courriel, il n'existait aucune collecte de renseignements personnels comme tel. Par conséquent, la plainte concernant la collecte abusive de renseignements personnels n'était pas fondée.

Toutefois, l'enquête a révélé que J.J. Barnicke n'avait pas en place de politiques ou procédures adéquates en matière de protection de la vie privée, ni ne comptait sur un agent désigné de la protection de la vie privée responsable de la conformité. Bien que J.J. Barnicke ait élaboré une telle politique durant l'enquête, la commissaire adjointe à la protection de la vie privée a recommandé que l'organisation affiche cette politique sur son site Web, distribue cette politique à ses employés et donne au personnel une formation adéquate concernant la protection de la vie privée. J.J. Barnicke a pleinement mis en œuvre les recommandations de la commissaire adjointe.

Le plaignant s'est adressé à la Cour fédérale. Il y eu ajournement d'une audience prévue pour novembre 2007 en raison d'une motion de procédure préliminaire, sans toutefois qu'une nouvelle date d'audience n'ait été fixée.

## Fonction de surveillance

Dans le cadre de notre rôle de surveillance des décisions judiciaires au sens large, le Commissariat à la protection de la vie privée continue de surveiller certaines affaires judiciaires impliquant de nouvelles questions d'actualité au chapitre de la protection de la vie privée. C'est l'une des façons par lesquelles nous demeurons au fait des progrès de droit réalisés, que ce soit au moyen de demandes en vertu de la *LPRPDE*, de la *Loi sur*

X. c. *Telus Communications Inc.*  
N° de dossier de la Cour d'appel fédérale : A-639-05

Cette affaire impliquait des plaintes d'employés de Telus sur la mise en œuvre par la compagnie d'un système de reconnaissance vocale.

En janvier 2007, la Cour d'appel fédérale confirmait

Note : Nous avons également  
relaté cette affaire dans nos  
rapports annuels de 2004, 2005  
et 2006.

- (i) L'empreinte vocale recueillie par Telus constitue des renseignements personnels.
- (ii) Dans les faits, une personne raisonnable trouverait raisonnable dans les circonstances qu'une entreprise adopte une technologie d'empreinte vocale à des fins d'authentification et de sécurité.
- (iii) Ce système d'authentification par empreinte vocale de Telus répond aux prescriptions de la *LPRPD* en matière de consentement puisque les employés ne pouvaient être inscrits dans le système sans leur consentement actif.
- (iv) Aucune des exceptions énoncées dans l'article 7 de la *LPRPD* prévoyant la collecte sans consentement ne s'applique à la situation.
- (v) Telus a adéquatement informé ses employés des conséquences éventuelles s'ils refusaient d'accorder leur consentement.

X. c. *Scotia Capital Inc.*  
N° de dossier de la Cour fédérale : T-2181-05

En réponse à une demande d'un plaignant souhaitant accéder à ses renseignements personnels, Scotia Capital a remis au plaignant une copie de ses renseignements personnels, excluant toutefois ses talons de chèque de paye ou les registres de ses heures de travail.

Le plaignant prétendait que Scotia Capital invoquait de manière inappropriée des exceptions liées à de l'information provenant d'un tiers et à des documents protégés par secret professionnel. Par suite de notre enquête, l'entreprise a expédié des renseignements additionnels au plaignant.

La Cour fédérale a examiné la question de savoir si de telles notes contenaient les renseignements personnels de la personne ayant été examinée, et le cas échéant, s'il s'appliquait des exceptions aux termes de la *LPRPDE* permettant de refuser l'accès à de tels renseignements. Selon la Cour fédérale, les notes contenaient effectivement les renseignements personnels de la personne concernée, et les prétentions d'exception en vertu de la *LPRPDE* ne s'appliquaient pas. Par conséquent, elle a ordonné au médecin de donner accès aux notes.

Le médecin a interjeté appel de la décision. Devant la Cour d'appel fédérale, les questions en jeu étaient de savoir, premièrement, si les notes constituaient les renseignements personnels de la personne examinée ou le produit du travail du médecin; et deuxièmement, si les notes prises dans le contexte d'un examen médical indépendant surviennent dans le cours d'une activité commerciale visée par la *LPRPDE*.

La Cour d'appel fédérale a rendu sa décision en février 2008. On y lisait que :

- (i) Les notes prises par un médecin examinateur dans le cadre d'un examen médical indépendant à la demande d'une compagnie d'assurance sont consignées au « cours d'une activité commerciale », de sorte qu'elles sont clairement visées par la *LPRPDE*.

- (ii) Les notes prises par un médecin examinateur dans le cadre d'un examen médical indépendant contiennent clairement des renseignements sur la santé d'une personne, et par voie de conséquence, des renseignements personnels.

La Cour d'appel fédérale a soutenu que la personne avait le droit d'accéder aux parties des notes qui contenaient des renseignements fournis par elle, et de corriger toute erreur que l'examinateur médical pourrait avoir faite.

Toutefois, le tribunal en a également déduit que les renseignements dans les notes pouvaient être personnels à la fois pour la personne et le médecin, et qu'il pourrait être nécessaire de parvenir à un équilibre en prenant en considération les intérêts privés de la personne et ceux du médecin, ainsi que l'intérêt public associé à la communication et à la non-communication.

On a retourné l'affaire à la commissaire à la protection de la vie privée de manière à ce qu'elle puisse, de concert avec l'avocat du médecin, déterminer les parties des notes qui contiennent les renseignements personnels de la personne et qu'il faudrait communiquer.

La commissaire à la protection de la vie privée a indiqué qu'elle prévoit revoir la question avec le ministre de l'Industrie dans le cas où il faudrait modifier la *LPRPDÉ* par suite d'une décision de la Cour suprême.

*X. c. Accusearch Inc., s/n Abika.com et autres*  
N° de dossier de la Cour fédérale : T-2228-05

Une personne a fait une demande de contrôle judiciaire pour obtenir une ordonnance d'annulation ou de cassation de la décision de la commissaire adjointe à la protection de la vie privée, qui affirmait ne pas disposer du pouvoir de faire enquête sur une plainte contre Accusearch Inc., une organisation américaine faisant affaire sous le nom d'Abika.com.

La personne souhaitait qu'on examine la position de la commissaire adjointe selon laquelle elle estimait ne pas avoir la compétence voulue pour faire enquête. En février 2007, la Cour fédérale a accueilli la demande en s'appuyant sur le fait que la commissaire adjointe avait la compétence voulue pour faire enquête sur la circulation transfrontalière des renseignements personnels dans un tel cas.

Il s'agit d'une décision importante pour le Commissariat en ce qu'elle a aidé à renforcer nos activités d'engagement internationales afin de mieux protéger les renseignements personnels des Canadiennes et Canadiens.

Par suite de cette décision, nous enquêtons sur la plainte contre Accusearch.

De plus, des poursuites ont été intentées aux États-Unis contre Accusearch en ce qui a trait à la publicité et à la vente de dossiers d'appels téléphoniques confidentiels à des tiers sans le consentement des personnes concernées. Étant donné l'intérêt grandissant du Commissariat pour les activités internationales aidant à protéger les renseignements personnels des Canadiennes et Canadiens, nous surveillons ces poursuites de près.

***Demandes au tribunal déposées par le plaignant en vertu de l'article 14 de la LPRPDÉ***  
*D. Jeffrey Wynndorwe (Psychiatric Assessment Services Inc.) c. X.*  
N° de dossier de la Cour d'appel fédérale : A-551-06

Il s'agit d'une affaire qui dure depuis longtemps, et dont nous avons discuté dans nos rapports annuels de 2005 et 2006. La question en jeu est de savoir si une personne a le droit d'accéder à ses renseignements personnels contenus dans des notes prises par un médecin lorsqu'il effectue un examen médical indépendant au nom d'une compagnie d'assurance.



## ***Demandes de contrôle judiciaire en vertu de l'article 18.1 de la Loi sur les Cours fédérales***

*Blood Tribe Department of Health c. commissaire à la protection de la vie privée du Canada et autres*

N° de dossier de la Cour suprême du Canada : 31755

Nous avons relaté les détails de cette affaire en cours dans nos trois derniers rapports annuels. En jeu se trouvent le secret professionnel qui lie un avocat à son client et notre capacité d'obtenir les renseignements dont nous avons besoin pour mener nos enquêtes. Le résultat final – qui reste à venir – aura des répercussions profondes sur la manière dont nous menons nos enquêtes.

L'affaire a débuté lorsqu'une femme ayant perdu son emploi au sein du Blood Tribe Department of Health a demandé son dossier personnel d'emploi, ce qu'on lui a refusé. Cette femme a porté plainte au Commissariat. Dans le cadre de notre enquête, nous avons demandé une copie du dossier personnel de la plaignante. Le Blood Tribe Department of Health a fourni certains registres, mais a fait valoir que les autres documents étaient protégés par le secret professionnel et a refusé de les remettre.

Nous étions d'avis qu'il nous fallait ces documents pour vérifier en toute indépendance si l'on pouvait soustraire à la communication les renseignements personnels demandés par une plaignante sous prétexte que ces renseignements sont protégés par le secret professionnel.

Nous avons rendu une ordonnance pour que l'organisation produise les documents. Le Blood Tribe Department of Health est allé devant le tribunal pour contester le pouvoir de la commissaire à la protection de la vie privée de rendre une telle ordonnance – ce qui a interrompu l'enquête.

La Cour fédérale a rejeté la demande de contrôle judiciaire du Blood Tribe Department of Health.

Toutefois, la Cour d'appel fédérale a annulé l'ordonnance de la commissaire à la protection de la vie privée, en s'appuyant sur le fait que le libellé de la *LPRPD* n'est pas suffisamment clair pour accorder à la commissaire le pouvoir particulier d'ordonner la production de documents protégés par le secret professionnel. La Cour nous a proposé de procéder en fonction de chaque cas lorsque nous voulons obtenir de la part de la Cour fédérale le droit d'examiner des documents protégés par le secret professionnel dans le contexte des plaintes impliquant un accès refusé à des renseignements personnels.

Nous avons porté cette décision en appel devant la Cour suprême du Canada, qui a prévu une audience le 21 février 2008.

Les parties ont réglé le différend. Air Canada a mis en œuvre les recommandations de la commissaire à notre satisfaction.

## Litiges en cours

Les litiges en cours ont trait à des demandes de contrôle judiciaire en vertu de l'article 18.1 de la *Loi sur les Cours fédérales* et à des demandes d'audience déposées par des plaignants en vertu de l'article 14 de la *LPRPD* dans laquelle le CPVP était impliqué comme partie ou comme intervenant.

Dans une affaire digne de mention, la State Farm Mutual Automobile Insurance Company a remis en question le pouvoir de la commissaire à la protection de la vie privée de faire enquête sur un refus de donner accès à des renseignements personnels et d'exiger la production de documents durant le déroulement de l'enquête.

En juillet 2007, State Farm a demandé une audience à la Cour du Banc de la Reine du Nouveau-Brunswick pour faire une déclaration selon laquelle :

- La *LPRPD* ne s'appliquait pas à la communication de renseignements personnels réclamés par un plaignant.
- La *LPRPD* a été édictée hors des pouvoirs attribués au Parlement fédéral.
- La commissaire à la protection de la vie privée n'avait pas le pouvoir de faire enquête sur la plainte en question.
- La commissaire à la protection de la vie privée n'avait pas le pouvoir d'exiger la production des renseignements demandés.

La commissaire à la protection de la vie privée a présenté une motion préliminaire pour que la demande de State Farm soit refusée ou mise en sursis en raison du fait que la Cour fédérale était le forum le plus indiqué.

La motion a été accueillie en janvier 2008 d'après le motif que la Cour fédérale était le forum le plus indiqué pour évaluer la demande, qui impliquait des questions de validité constitutionnelle et le contrôle judiciaire du pouvoir de la commissaire à la protection de la vie privée. L'appel de cette décision interjeté par State Farm sera entendu au début de 2008. De plus amples renseignements seront fournis dans notre prochain rapport annuel.

D'autres décisions judiciaires importantes rendues en 2007 apparaissent ci-dessous.

*X. c. ING Canada Inc.*  
N° de dossier de la Cour fédérale : T-1283-07

Un plaignant a fait une demande de contrôle judiciaire en vertu de l'article 18.1 de la *Loi sur les Cours fédérales*. Le CPVP a amorcé un processus de médiation, et par suite d'une entente négociée, le plaignant a retiré sa demande.

*X. c. Brampton Flying Club*  
N° de dossier de la Cour fédérale : T-192-05

Un plaignant a demandé une audience en vertu de l'article 14 parce qu'il alléguait que Brampton Flying Club avait négligé de lui donner accès à ses renseignements personnels dans les 30 jours suivant sa demande écrite et qu'on avait tenté de lui imposer un montant déraisonnable pour répondre à sa demande. Cette affaire a été réglée par les parties en janvier 2007.

*X. c. Laidlaw Transit Ltd.*  
N° de dossier de la Cour fédérale : T-684-07

Un plaignant a demandé une audience en vertu de l'article 14 pour contester une forme de surveillance en milieu de travail entreprise par Laidlaw Transit Ltd. Le CPVP a servi de médiateur dans le différend. Le plaignant a renoncé à sa demande, et les parties sont parvenues à une entente.

*X. c. La Banque de Nouvelle-Écosse*  
N° de dossier de la Cour fédérale : T-2126-05

Cette affaire concernait une plainte selon laquelle un ou plusieurs employés de la Banque de Nouvelle-Écosse avaient obtenu des renseignements personnels sans consentement et communiqué ces renseignements à un tiers. Le plaignant a renoncé à sa demande d'audience devant la Cour fédérale, et l'affaire a été réglée entre les parties.

*Commissaire à la protection de la vie privée du Canada c. Air Canada*  
N° de dossier de la Cour fédérale : T-342-07

La commissaire à la protection de la vie privée a demandé une audience à la Cour fédérale afin d'amener Air Canada à mettre en œuvre ses recommandations dans une affaire portant sur l'ampleur des renseignements médicaux personnels recueillis par l'organisation lorsqu'elle voulait s'assurer de la capacité d'un employé de retourner au travail.

La commissaire à la protection de la vie privée peut tenter des poursuites lorsqu'une organisation refuse d'adopter ses recommandations dans des cas fondés, ce qui a aidé à établir un niveau élevé de conformité aux recommandations.

En vertu de l'article 14 de la *LPRPD*, un plaignant ou la commissaire à la protection de la vie privée peut, dans certaines circonstances, demander une audience à la Cour fédérale pour toute question évoquée dans le rapport de la commissaire.

L'article 15 permet également à la commissaire à la protection de la vie privée, avec le consentement du plaignant, de demander directement une audience à la Cour fédérale concernant une affaire visée par l'article 14. Conformément à cet article, la commissaire peut comparaître devant la Cour fédérale au nom de tout plaignant ayant demandé une audience en vertu de l'article 14. Elle peut également, avec la permission de la Cour fédérale, comparaître comme partie à toute audience en vertu de l'article 14 non demandée par elle-même.

Depuis notre compte rendu de la situation des procédures en cours dans notre rapport annuel de 2006 sur la *LPRPD*, de nouvelles demandes ont été produites, et certains litiges ont été résolus. Nous discutons ci-dessous de ces nouveaux développements.

Conformément à la lettre et à l'esprit de notre mandat, nous avons respecté la vie privée des plaignants en retirant leur nom.

## Causes réglées

En 2007, plusieurs demandes de nature judiciaire déposées contre des organisations ont été réglées avant que la Cour fédérale ne les ait entendues et qu'elle n'ait rendu une décision.





## Vérifications d'Equifax et de TransUnion

La commissaire à la protection de la vie privée a complété des vérifications simultanées des systèmes d'identification et d'authentification en ligne des agences d'évaluation du crédit Equifax Canada et TransUnion.

La société Equifax a entrepris une poursuite dans le cadre de laquelle elle remettrait en question l'existence de motifs raisonnables justifiant la décision de la commissaire à la protection de la vie privée de procéder à une vérification. Bien qu'Equifax ait maintenu tout au long du processus que la vérification ne reposait pas sur des motifs raisonnables, la vérification a été conclue. Un rapport a été remis à Equifax, et aucune autre mesure n'était requise de la part d'Equifax par suite de cette vérification.

TransUnion estimait également que la commissaire n'avait pas de motifs raisonnables, mais a choisi de ne pas tenter de poursuivre. Comme ce fut le cas avec la vérification d'Equifax, TransUnion a reçu un rapport et aucune autre mesure n'était requise de sa part par suite de cette vérification.

## Outil d'auto-évaluation

Le Commissariat prépare un outil pour aider les organisations à évaluer leur conformité à la *LPRPD* et à ses principes relatifs à l'équité dans le traitement des renseignements. Cet outil aidera les organisations à diagnostiquer les problèmes posés par leurs systèmes et pratiques de protection de la vie privée.

Nous sollicitons des observations sur ce nouvel outil d'auto-évaluation de plusieurs responsables de la protection des renseignements personnels des grandes entreprises, de professeurs d'université, de chefs de file en formation et perfectionnement des gestionnaires ainsi que d'associations de gens d'affaires et d'associations professionnelles. Nous nous attendons à disposer en 2008 d'une version finale pour les moyennes et grandes entreprises.

# Comment décidons-nous s'il y a lieu de faire une vérification en vertu de la LPPDE?

Le Plan stratégique et le Rapport annuel sur les plans et les priorités du Commissariat décrivent les résultats que nous voulons obtenir. Tout au long du processus visant à déterminer s'il y a lieu de mener une vérification, nous prenons en considération le mandat, les objectifs, les plans et les priorités du Commissariat.

## Plans stratégiques

Action	Motifs	Analyse des enjeux
<p>PRINCIPE 3 : Compte tenu des résultats de l'analyse des enjeux et du processus d'établissement des motifs raisonnables, quelles mesures permettraient le milieu de promouvoir et d'encourager la conformité et l'application de saines pratiques de gestion des renseignements personnels? La vérification est-elle la meilleure approche et le secteur examine-t-il bien à une vérification?</p> <p>Le Commissariat reconnaît qu'aucun outil ou instrument ne suffit à lui seul à faire respecter la conformité dans toutes les situations. C'est pourquoi il examine tous les moyens à sa disposition, y compris la vérification, pour encourager la conformité et promouvoir de saines pratiques de gestion des renseignements personnels. La décision finale de procéder à une vérification dépend de nombreuses considérations comme la nature de l'affaire, l'importance des risques systémiques, la fréquence à laquelle le problème a été observé, l'ampleur des mesures correctives prises, les résultats et les conclusions des enquêtes terminées et en cours sur la protection des renseignements personnels et les positions antérieures du Commissariat.</p>	<p>PRINCIPE 2 : Existe-t-il des preuves suffisantes et crédibles indiquant une forte possibilité qu'une vérification révèle une contravention à la Loi?</p> <p>Ce qui constitue un motif raisonnable repose sur l'examen de l'information recueillie durant les activités d'analyse des enjeux et sur le processus visant à décider s'il existe des motifs suffisants pour justifier que le Commissariat exerce son pouvoir discrétionnaire en vertu du paragraphe 18(1) de la Loi. À l'interne, le CVP établit des fondements clairs pour la vérification et s'assure que le seuil de preuve est adéquat.</p>	<p>PRINCIPE 1 : Existe-t-il des facteurs, ou s'est-il produit des incidents, qui indiquent un risque de non-conformité à la Loi ou l'absence de saines pratiques de gestion de la protection des renseignements personnels?</p> <p>Ce processus comprend la détermination, l'analyse et la confirmation des enjeux relatifs à la protection des renseignements personnels d'une entité ou d'un programme, et si possible, un examen préliminaire des principales fonctions de contrôle de la gestion des renseignements personnels. L'analyse des enjeux est généralement menée à l'interne et basée sur de l'information recueillie par le CVP au moyen d'enquêtes et de recherches, mais elle peut comporter plusieurs interventions, y compris des enquêtes auprès de la direction. Voici certains des facteurs qui peuvent indiquer l'absence de saines pratiques de gestion des renseignements personnels : rapports crédibles des médias, recommandations de comités parlementaires, contraventions révélées par des dénonciations, enquêtes sur un incident, résultats d'enquêtes sur des plaintes, demande d'examen d'une entité ou de l'industrie, résultats d'études empiriques ou sondages dans l'industrie.</p>

Dossier indiquant les critères sur lesquels se base le Commissariat pour décider de procéder à une vérification.

Les vérifications représentent l'un des outils de conformité prévus par la *LPRPDE*. La commissaire à la protection de la vie privée a le pouvoir de vérifier les pratiques d'une organisation en ce qui touche la gestion des renseignements personnels dans les cas où elle a des motifs raisonnables de croire que ces pratiques ne sont pas conformes à la Loi. Lorsqu'une vérification est amorcée en vertu de la *LPRPDE*, le vérificateur dispose du pouvoir délégué de recevoir des preuves des témoins, de pénétrer dans un local à toute heure raisonnable, et d'examiner des registres trouvés sur les lieux ou d'obtenir des copies de tels registres. Au besoin, la commissaire à la protection de la vie privée peut obliger des gens à fournir des preuves.

Au terme d'une vérification, nous fournissons à l'organisation un rapport de nos conclusions et toute recommandation que la commissaire estime appropriée. Le rapport peut être divulgué s'il en va de l'intérêt du public.

Le Commissariat réalise également des vérifications auprès des institutions fédérales assujetties à la *Loi sur la protection des renseignements personnels*.

Le but des vérifications – dans le secteur privé comme dans le secteur public – consiste à promouvoir la responsabilité et la conformité aux lois, politiques et normes applicables, et aussi à contribuer à l'amélioration des systèmes et pratiques de protection de la vie privée.

## Cadre pour amorcer des vérifications en vertu de la *LPRPDE*

L'une des questions les plus fréquemment posées par les organisations assujetties à la *LPRPDE* pourrait être : Sur quoi vous fondez-vous pour mener ou non une vérification? La décision de mener ou non une vérification est prise en fonction de chaque cas. La loi exige de la commissaire d'avoir des motifs raisonnables de croire qu'il y a non-conformité à la Loi pour mener une vérification.

En 2007, nous avons élaboré un cadre pour amorcer des vérifications qui donne un certain aperçu du processus de sélection des vérifications.

sociale et de compte. L'entreprise a avisé les personnes concernées et instauré des alertes sur les comptes des clients touchés.

- Il y a eu vol de l'ordinateur portatif d'un employé d'une agence faisant la promotion d'un événement dans un casino. L'ordinateur portatif, qui était dans une voiture lors du vol, contenait une base de données protégée par un mot de passe et contenant de l'information sur certains des participants à l'événement, sauf que les données n'étaient pas cryptées. Les renseignements personnels incluaient le nom et l'âge des participants, leurs coordonnées, les numéros de leurs permis de conduire et, dans un cas, les numéros du passeport et de la carte Santé. Par suite de l'incident, l'agence a informé les personnes touchées et leur a offert des arrangements pour la surveillance du crédit. Elle a également adopté plusieurs mesures de sécurité, comme des logiciels cryptographiques sur les ordinateurs portatifs, et a rappelé aux employés les politiques et procédures de sécurité. L'employé responsable de la perte des données a été congédié.

Nous espérons que la sensibilisation croissante des gens à la nécessité d'informer le Commissariat et les personnes touchées lorsqu'il se produit une atteinte à la vie privée se traduira sous peu en mesures de sécurité plus efficaces. Nous continuons à exhorter les particuliers comme les organisations à prendre des précautions de base pour sécuriser les données, par exemple :

- Limiter la quantité de renseignements personnels recueillis, utilisés et transportés par le truchement de dispositifs électroniques.
- Ne jamais laisser sans surveillance un ordinateur portatif dans des situations où on pourrait le dérober.
- Utiliser des technologies qui rehaussent le niveau de sécurité et de protection de la vie privée telles que les services de chiffrement des données et de préservation de l'anonymat.
- Utiliser des mots de passe difficiles à trouver.
- Éviter le recours aux caractéristiques d'accès automatique qui sauvegardent les noms et mots de passe.
- S'assurer que les renseignements personnels dans un disque dur sont entièrement écrasés — pas seulement effacés — avant de jeter au rebut ou de vendre un ordinateur.

En suivant ces étapes, les organisations peuvent considérablement réduire le risque de compromission des renseignements personnels qu'elles détiennent.

touchés – ce qui découle en partie de l'élaboration et de la publication de nos lignes directrices sur les atteintes à la sécurité des données.

Les organisations ont volontairement déclaré 34 atteintes en 2007, par rapport à 20 l'année précédente. Les atteintes à la sécurité des données signalées par l'intéressé en 2007 ont compromis les renseignements personnels de quelque 50 000 personnes.

Bien que différents secteurs commencent à nous signaler des atteintes à la sécurité des données, notamment des groupes de recherche et des compagnies publicitaires, l'essentiel de ces avis continue de provenir des industries du domaine bancaire, des télécommunications et du commerce de détail.

Il vaut la peine de mentionner que la moitié des atteintes qui nous ont été rapportées avaient trait à des données électroniquement stockées – c'était souvent le fait de renseignements sur les consommateurs stockés dans des ordinateurs portatifs volés. De plus, nous avons découvert que près de neuf personnes sur dix touchées par une atteinte déclarée par l'intéressé se trouvaient en situation de risque étant donné que leurs renseignements personnels étaient détenus sur support électronique non sécurisé ou non doté de mécanismes de protection comme des coupe-feu et des procédés de cryptage.

Nous nous réjouissons de constater que les organisations nous faisant des déclarations volontaires agissent en temps opportun – souvent moins d'un jour ou deux suivant l'incident. Un avis rapide nous aide à nous préparer aux demandes de renseignements des médias ou aux plaintes qui suivent l'avis expédié aux personnes touchées. La déclaration volontaire nous permet également de recueillir des statistiques et de sensibiliser les organisations et le public sur les causes des atteintes à la sécurité des données ainsi que sur les mesures préventives recommandées.

Voici de brèves descriptions de certaines atteintes rapportées au Commissariat en 2007 :

- L'employé d'une firme sous contrat avec une institution financière s'est fait voler son ordinateur portable à son domicile. L'ordinateur contenait les renseignements personnels de plusieurs centaines d'employés, sauf que ces renseignements n'étaient pas considérés comme délicats. L'institution financière et la firme sous contrat avaient en place des contrôles pertinents pour protéger les renseignements personnels, mais l'employé ne les a pas appliqués. Par suite de cet incident, l'établissement a mis en place des contrôles additionnels tels que des logiciels de chiffrement.

- Un voleur s'est emparé d'un ordinateur portable dans le véhicule d'un employé d'une société de services financiers. Cet ordinateur contenait des registres de la clientèle. Plus de la moitié de ces registres révélaient des numéros d'assurance



Toutefois, il a été constaté en voyant que les courriels expédiés par la compagnie à ces autres personnes étaient conçus de manière à donner l'impression qu'ils provenaient de lui-même. Plus particulièrement, il était renversé de voir que son ex-épouse avait reçu un courriel dans lequel il donnait censément à entendre que les deux voyageraient ensemble s'il gagnait le concours.

Il s'est plaint du fait qu'on s'était servi de son nom dans les courriels sans son consentement. La commissaire adjointe à la protection de la vie privée a conclu que la plainte n'était pas fondée. Les règles du concours et leur formulation indiquaient clairement que les messages par courriel aux personnes en référence seraient personnalisés comme si le concurrent les avait lui-même expédiés. Étant donné que le prix consistait en un voyage pour quatre personnes, elle a estimé raisonnable de s'attendre à ce que le message suggère que l'abonné et le destinataire du courriel voyageraient ensemble.

## Enquêtes sur des incidents

Le Commissariat mène également des enquêtes sur des incidents ayant trait à des violations possibles de la *LPRPDE*. Nous recevons des rapports de déclaration volontaire d'incidents de la part d'organisations, des rapports des médias sur des atteintes possibles à la sécurité des données, et de l'information de gens qui aimeraient que nous nous penchions sur un dossier, mais qui ne sont pas nécessairement touchés par l'affaire.

Entre autres exemples d'incidents du genre, mentionnons des reçus de carte de crédit trouvés dans des bennes à rebuts ou des rapports d'atteintes à la sécurité de l'information sur les sites Web.

Lorsqu'on porte un incident à notre attention, nous travaillons avec l'organisation responsable à corriger toute lacune et résolvons les affaires restantes telles que l'envoi d'avis aux clients touchés, l'extraction de l'information, et l'assurance que sont mises en oeuvre des mesures de sécurité appropriées.

En 2007, nous avons mené 12 enquêtes sur des incidents portés à notre attention d'une source autre que l'organisation directement impliquée dans l'incident.

## Déclaration volontaire d'atteintes à la sécurité des données

Malgré le fait que les lois relatives à la protection des renseignements personnels existent depuis plusieurs années, ce ne sont pas toutes les organisations qui disposent de politiques et procédures claires concernant les atteintes à la sécurité des données. Cela dit, nous estimons que les gens sont davantage sensibilisés à la nécessité d'avertir le Commissariat des atteintes à la sécurité des données et aussi d'informer les clients

Elle a recommandé à la compagnie d'informer les clients dès le début de chaque appel de marketing sortant que la conversation serait enregistrée ou surveillée d'une autre manière et de leur expliquer pourquoi elle agit ainsi.

La compagnie de télécommunications a accepté de mettre en œuvre les recommandations.

### **Une station de télévision agit de manière à enregistrer secrètement les appels d'une employée**

Un syndicat représentant les employés d'une station de télévision dans une petite communauté a allégué qu'un gestionnaire avait installé de l'équipement d'enregistrement des appels téléphoniques dans le poste de travail d'une représentante du service à la clientèle. La station aurait enregistré sur ruban ses conversations téléphoniques sans sa connaissance et son consentement.

L'enquête a confirmé la véracité de l'allégation. Nous avons extrait d'un dossier dans l'ordinateur de la plaignante une conversation enregistrée entre elle et son conjoint. La plaignante nous a dit quelle ne savait pas que l'appel était enregistré.

Interrogé, l'employeur a soutenu que l'équipement n'était pas encore opérationnel et qu'on l'avait installé pour faire un essai, dans l'intention d'enregistrer des conversations au cas où surviendrait un désaccord de facturation ainsi que pour dissuader les clients injurieux.

Puisque la station avait l'intention d'installer un tel équipement dans tous les postes de travail des représentants du service à la clientèle, la commissaire adjointe lui a recommandé d'informer à l'avance les employés de ses plans et de l'objectif poursuivi. Elle lui a également indiqué quelle devait informer ses clients que leurs appels pouvaient être enregistrés et leur expliquer la raison d'une telle démarche.

On a considéré que la plainte était fondée et résolue. La station a décidé en bout de ligne de ne pas enregistrer les appels.

### **Les règles d'un concours comportaient un avertissement adéquat selon lequel il y aurait partage des adresses de courriel**

Un abonné du bulletin d'une entreprise s'est inscrit à son concours afin de gagner des vacances pour quatre personnes. Il a fourni les adresses de courriel d'autres personnes de manière à avoir plusieurs inscriptions au concours.

## Un agent d'assurance communiqué de l'information sans consentement approprié

Une personne s'est plainte du fait qu'un administrateur de prestations d'assurance médicale avait communiqué de manière inappropriée des renseignements personnels délicats à son employeur, en dépit du fait qu'elle avait signé un formulaire de consentement limité en matière de communication de renseignements.

Au moment de faire une demande de prestations d'invalidité de longue durée, la personne en cause a négocié une entente de consentement à diffusion restreinte avec l'évaluateur de la compagnie d'assurance dans le but exprès de restreindre le droit de l'assureur de transférer les renseignements médicaux à son employeur.

Des mois plus tard, une agente en réadaptation pour le compte de compagnies d'assurance, dont l'employeur du plaignant avait retenu les services, croyait avoir le consentement verbal du plaignant pour informer son employeur qu'il était prêt à retourner au travail.

Elle a donc expédié par courriel à l'employeur des extraits du rapport d'un spécialiste médical – même si le plaignant lui avait rappelé les instructions du consentement limité. La commissaire à la protection de la vie privée en a déduit que la communication de renseignements n'était pas appropriée et qu'il aurait fallu obtenir le consentement écrit. La commissaire a recommandé à la compagnie de mettre à jour ses politiques et sa formation. La compagnie a suivi ces recommandations.

## Une compagnie de télécommunications néglige d'obtenir le consentement l'autorisant à enregistrer les appels

Une personne s'est plainte du fait qu'une compagnie de télécommunications n'obtenait pas le consentement approprié avant d'enregistrer ses appels sortants.

La compagnie avait téléphoné à la mère du plaignant, mais ne l'avait pas informée qu'elle enregistrerait l'appel. La politique de la compagnie exige des employés qu'ils informent les gens de l'enregistrement des appels entrants, mais non sortants.

Selon la compagnie, une déclaration dans sa politique écrite sur la protection de la vie privée était un moyen suffisant d'obtenir le consentement l'autorisant à enregistrer les appels sortants, ce avec quoi n'était pas d'accord la commissaire à la protection de la vie privée.

## CAS PRÉSENTANT DE L'INTÉRÊT

*Dans la partie suivante, on trouve un échantillon de cas sur lesquels nous avons travaillé en 2007 qui ont une importance systémique pour les enjeux liés à la protection de la vie privée au Canada.*

### Une décision judiciaire entraîne une enquête transfrontalière

Une décision de la Cour fédérale prise en février 2007 a annulé une décision de la commissaire à la protection de la vie privée selon laquelle elle n'avait pas la juridiction voulue en vertu de la *LPDP* pour faire enquête sur une plainte contre un courtier en données installé aux États-Unis, Accusearch Inc., et fonctionnant sous le nom d'Abika.com.

Par suite de cette décision, le Commissariat mène une enquête sur une plainte déposée par un particulier contre Accusearch. Dans le cadre de notre enquête, nous avons contacté la Federal Trade Commission des États-Unis, avec qui nous discutons activement de la manière de travailler conjointement sur des dossiers ayant trait à Accusearch.

### Numéro de carte de crédit imprimé sur un billet d'avion

Un client d'une agence de voyage ayant acheté un billet d'avion a été troublé de constater qu'on avait transféré à un grossiste les renseignements figurant sur sa carte de crédit, et que le numéro complet de sa carte de crédit, y inclus la date d'expiration, était imprimé sur son billet.

La commissaire a recommandé à l'agent de voyage de mieux informer ses clients du fait que leurs renseignements personnels seraient transférés aux grossistes. En outre, elle a recommandé à l'agence de confirmer les pratiques du grossiste en matière de manipulation des renseignements, car elle avait constaté que le grossiste hésitait à révéler ses pratiques – bien qu'il existait un contrat afférent entre les deux parties.

L'agence a plus tard informé le Commissariat qu'elle ne ferait plus affaire avec le grossiste. Jusqu'à ce que cesse complètement la production de billets en papier (en décembre 2007), la commissaire a recommandé à l'agence d'expliquer aux clients que les renseignements sur la carte de crédit apparaîtraient sur les billets en papier. En outre, l'agence doit leur offrir l'option d'un billet électronique, qui ne contient pas ces renseignements.

communiquer de l'information confidentielle dans les cas particuliers présumés et/ou dans des cas types ultérieurs. L'ingénierie sociale implique la manipulation des gens pour obtenir d'eux des renseignements personnels, par exemple en prétendant être une personne autorisée à obtenir l'information.

Le commissaire adjoint en a déduit que les procédures d'authentification des compagnies et la formation du personnel ne suffisaient pas à protéger adéquatement les renseignements du consommateur ou à répondre aux prescriptions de la *LRPDE*.

Il a également été préoccupé par le fait que les compagnies n'en avaient pas fait suffisamment pour prévenir les employées des tactiques utilisées par les courtiers en données — même si des incidents survenus aux États-Unis avaient déjà soulevé des préoccupations.

Bien que le commissaire adjoint se soit réjoui du fait que les trois compagnies avaient revu leurs procédures d'authentification de la clientèle peu après la mise au jour des communications de renseignements, il a recommandé d'autres changements en ce qui touche la formation du personnel ainsi que les procédures relatives à l'authentification et à la communication de renseignements personnels.

Les compagnies ont mis en œuvre toutes ces mesures, sauf une, pour laquelle elles ont proposé des solutions de rechange que le commissaire adjoint a trouvées acceptables. Par conséquent, il a jugé que les plaintes étaient fondées et résolues.

Le commissaire adjoint a pris note du fait que les organisations doivent adapter leurs politiques et pratiques en matière de renseignements personnels à mesure que continuent de se poser et d'évoluer les menaces aux renseignements personnels.

Au départ, le commissaire adjoint avait également déposé une plainte contre Locatecell. Toutefois, les résultats préliminaires de nos demandes de renseignements ont révélé que nous n'avions pas la juridiction voulue pour poursuivre l'enquête.

Dans la foulée de ces incidents et des poursuites contre les courtiers en données aux États-Unis, les activités des courtiers ont pris fin ou ont été radicalement restreintes. Bon nombre de sites Web de courtiers ne sont pas accessibles, et celui de Locatecell.com ne fonctionne plus depuis quelque temps.



Au Canada, la SWIFT recueille des renseignements personnels des banques canadiennes et lui en communique également à des fins de paiements transfrontaliers, de compensation et de règlements de valeurs mobilières et de services de trésorerie et de commerce. Sa présence au Canada est importante. La grande majorité des transferts internationaux touchant la circulation de renseignements personnels depuis et vers des institutions financières canadiennes s'effectuent au moyen du réseau de la SWIFT.

Au terme d'une enquête, la commissaire a conclu en avril 2007 que la SWIFT était assujettie à la *LPRPDE*, mais quelle ne l'avait pas enfreinte.

La commissaire a pris en note le fait que la loi permet à des organisations telles que la SWIFT de respecter les lois légitimes des autres pays où elles mènent des activités. Elle a également retenu que l'exception prévue par la *LPRPDE* en matière de connaissance ou de consentement s'applique à une organisation communiquant des renseignements personnels lorsqu'il y a délivrance d'une assignation à témoigner licite.

Dans l'affaire qui nous intéresse, le département du Trésor des États-Unis a commencé à délivrer des assignations à comparaître à la SWIFT en raison des données détenues dans son centre d'exploitation situé en terre américaine par suite des attaques terroristes du 11 septembre 2001.

Dans ses conclusions, la commissaire a indiqué que, si les autorités américaines avaient besoin de renseignements sur des transactions financières du côté canadien, il faudrait les inviter à utiliser les mécanismes d'information existants qui offrent un certain degré de transparence et des protections intégrées pour protéger la vie privée, comme les mécanismes canadiens de lutte contre le recyclage des produits de la criminalité et le financement des activités terroristes.

## Affaire des télécommunications : Mise en lumière de l'importance de l'authentification

Le commissaire adjoint à la protection de la vie privée, Raymond D'Aoust, a déposé des plaintes contre trois compagnies canadiennes de télécommunications par suite de la publication en novembre 2005 d'un article dans le *Maclean's* décrivant la façon dont le magazine avait obtenu les relevés d'appels téléphoniques de la commissaire à la protection de la vie privée.

Les relevés avaient été achetés d'un courtier en données américain, Locatecell.com, qui les avait obtenus de Bell, TELUS Mobilité et Fido.

L'enquête a révélé que Locatecell.com avait eu recours à l'« ingénierie sociale » pour persuader des représentants du service à la clientèle des compagnies téléphoniques de

Nous nous engageons à réduire les délais de traitement et à éliminer l'arrière de cas sur lesquels enquêter sans compromettre la qualité du travail. À cette fin, le Commissariat continue à mettre en place des mesures novatrices.

Les changements mis en œuvre ces dernières années, y compris l'embauche et la formation de nouveaux employés, ont aidé à donner un nouveau souffle à notre section chargée des enquêtes. Nous prévoyons améliorer davantage la prestation des services par les moyens suivants :

- Poursuivre les mesures d'embauche.
- Accroître l'automatisation et l'utilisation de la technologie dans le traitement des dossiers.
- Rationaliser nos processus d'enquête.

Tout ce travail est essentiel pour préserver la confiance renouvelée des Canadiennes et Canadiens envers le Commissariat et sa capacité de protéger le droit à la protection de la vie privée. Le traitement équitable, rapide et efficace des plaintes offre une occasion clé de sensibiliser le secteur privé et la population canadienne.

## Plaintes déposées par la commissaire

La commissaire utilise ses pouvoirs pour déposer des plaintes sur un vaste éventail d'enjeux concernant la protection de la vie privée. Ci-dessous apparaît le sommaire de deux plaintes importantes déposées par la commissaire et résolues en 2007.

### Affaire SWIFT : La circulation transfrontalière de données pose de nouveaux risques à la protection de la vie privée

En août 2006, la commissaire a la protection de la vie privée a lancé une enquête après la parution de reportages dans les journaux selon lesquels la Society for Worldwide Interbank Financial Telecommunication (SWIFT) avait communiqué au département du Trésor des États-Unis des dizaines de milliers de registres contenant des renseignements personnels.

Les documents communiqués contenaient des renseignements personnels provenant d'institutions financières canadiennes ou transférés à celles-ci. Ils incluaient vraisemblablement des données telles que les noms, adresses et numéros de compte ainsi que les sommes transférées.

y avait violation de la *LPRPDE*, mais la partie intimée a accepté d'appliquer nos recommandations.

On dira d'une plainte ayant fait l'objet d'une enquête complète que'elle est soit fondée, soit fondée et résolue, selon le niveau de coopération reçue de la partie intimée.

Une plainte est considérée comme fondée lorsque la commissaire est d'avis qu'il y a vraisemblablement eu violation de la *LPRPDE*. Elle prépare un rapport préliminaire assorti de recommandations concernant des mesures correctives que devrait appliquer la partie intimée, qui a 30 jours pour répondre à ce rapport.

Ce processus de rapport préliminaire établi en 2006 s'est révélé un moyen efficace de s'assurer que les organisations demeurent responsables.

Si la partie intimée se conforme aux recommandations, on parle habituellement d'une plainte fondée et résolue. Dans les cas où la partie intimée ne se conforme pas intégralement, la plainte est considérée comme étant fondée.

En 2007, nous avons produit des rapports préliminaires pour 38 plaintes résolues. De ce nombre, 34 organisations se sont conformées aux recommandations de la commissaire.

En 2007, seulement quatre organisations ont choisi de ne pas mettre en œuvre nos recommandations au terme de l'enquête. Dans de tels cas, la commissaire a de façon constante cherché à faire confirmer ses recommandations par la Cour fédérale.

Au moment où nous nous préparions à publier ce rapport annuel, les quatre organisations qui avaient initialement refusé d'adopter nos recommandations avaient finalement accepté de se conformer, soit avant ou après que nous ayons renvoyé les causes au contentieux.

## Délais de traitement

Le délai de traitement moyen (calculé à partir de la date où la plainte est reçue jusqu'à la date où le rapport des conclusions est mis à la poste) des plaintes en vertu de la *LPRPDE* résolues en 2007 était de 15,7 mois – à peu près le même qu'en 2006.

Fait plus positif, seulement 44 dossiers étaient en suspens – non attribués parce qu'aucun enquêteur n'est disponible – à la fin de 2007. C'est beaucoup plus bas que les 76 dossiers en suspens de l'année précédente.

paramètres de la surveillance. En outre, ces organismes doivent élaborer des politiques précises concernant la surveillance, y compris l'enregistrement de tiers sur vidéo.

## Tendances au chapitre des plaintes

Nous avons résolu 420 plaintes en 2007. La grande majorité d'entre elles (39 p. 100) concernait des questions d'utilisation et de communication de renseignements personnels, une tendance observée ces dernières années. À l'image des années précédentes, d'autres types courants de plaintes avaient trait à la collecte (19 p. 100) et à l'accès (16 p. 100).

Près du tiers (30 p. 100) des plaintes résolues en 2007 ont été réglées en cours d'enquête. Il s'agit de plaintes pour lesquelles le Commissariat a négocié un résultat satisfaisant pour toutes les parties, sans avoir eu à émettre de conclusions. En 2004, nous avons défini la catégorie « réglée en cours d'enquête » afin de faire le suivi de ce résultat.

En 2004, 40 p. 100 de nos cas ont été réglés en cours d'enquête. Toutefois, ce pourcentage a, par la suite, diminué de façon constante.

Cette tendance témoigne peut-être du fait que nous nous attaquons à des cas plus complexes nécessitant une enquête approfondie.

Plaintes résolues en 2007 – Par conclusions	
Pourcentage	
30	Réglées en cours d'enquête
21	Abandonnées
15	Non fondées
15	Fondées et résolues
10	Résolues
3	Réglées rapidement
3	Hors juridiction
2	Fondées

Un nombre appréciable de dossiers résolus ont été abandonnés en raison d'un désistement (21 p. 100) du plaignant ou du Commissariat. Cette donnée représente une hausse par rapport aux années précédentes. Comme ce fut le cas antérieurement, certains plaignants ont décidé pour des raisons personnelles d'abandonner leur plainte. D'autres n'ont pas poursuivi l'affaire parce qu'ils en sont arrivés à une entente avec l'organisation avant le début de l'enquête. D'autres, enfin, laissent tomber leur plainte à cause des délais de traitement prolongés. Parfois, le Commissariat doit abandonner des plaintes parce que les plaignants ne lui ont pas fourni les détails additionnels qu'il leur avait demandés et qui étaient nécessaires pour réaliser l'enquête.

Une fois les enquêtes complétées, 15 p. 100 des plaintes se sont révélées non fondées alors que les organisations s'étaient conformées à la *LPDP*. Une autre proportion de 15 p. 100 des plaintes étaient fondées et ont été résolues. En d'autres mots, il



## Plaintes par secteur

Comme c'est le cas depuis 2004, moment de la mise en œuvre intégrale de la *LPRPDE*, le secteur des institutions financières a été, en 2007, le plus souvent ciblé par les plaintes. Nous avons reçu 105 plaintes impliquant des institutions financières en 2007, ce qui représente près du tiers de toutes les plaintes formulées en vertu de la *LPRPDE*. Cette proportion est similaire à celle observée ces dernières années.

À l'image des années précédentes, les autres principaux secteurs de plaintes ont été les télécommunications, les assurances, les ventes et le transport. Toutefois, au cours des dernières années, nous avons constaté une diminution des plaintes impliquant des entreprises dans ces secteurs.

Nous avons enregistré une hausse régulière des plaintes concernant les services professionnels et les services d'hébergement. Toutefois, le nombre de plaintes contre ces secteurs demeure faible en comparaison des autres.

En ce qui concerne les plaintes impliquant l'industrie de l'assurance, on constate un nombre accru de dossiers où il est question de collecte clandestine de renseignements personnels par des firmes d'enquêteurs privés.

La *LPRPDE* comporte des dispositions où une compagnie d'enquête privée est désignée comme un « organisme d'enquête du secteur privé » qui assume des responsabilités précises en vertu de la Loi.

Nous comprenons l'éventuel besoin d'une collecte clandestine de renseignements personnels là où ont échoué d'autres efforts moins envahissants pour la vie privée. Cependant, ce type d'enquête soulève une grande préoccupation en raison du risque que des tiers innocents puissent être filmés en secret par des caméras de surveillance vidéo. Peu d'entre nous aimeraient être enregistrés sur vidéo en robe de chambre sur notre pertron avant simplement parce que nous sommes voisins d'une personne soupçonnée de fraude à l'endroit d'une compagnie d'assurance.

Nous travaillons avec des sociétés d'assurance et des organismes d'enquête privée afin de trouver un équilibre entre leur besoin de mener leurs affaires et le droit des gens à leur vie privée. Les compagnies d'assurance et leurs sous-traitants devraient utiliser la surveillance clandestine en dernier recours seulement. Les entreprises devraient s'assurer que la décision d'effectuer de la surveillance clandestine provient de la haute direction. Une partie de la solution pourrait être que les compagnies d'assurance établissent des contrats détaillés avec les organismes d'enquête où seraient clairement définis les



## Plaintes

En 2007, nous avons reçu 7 636 demandes reliées à la *LPRPDE*, ce qui représente une augmentation appréciable par rapport aux 6 050 demandes reçues l'année précédente. Nous avons constaté une hausse marquée de l'intérêt envers le vol d'identité et les sites de réseautage social comme Facebook.

En 2007, nous avons reçu 350 nouvelles plaintes en vertu de la *LPRPDE*. Ainsi, nous en avons reçu 424 en 2006, 400 en 2005 et 723 en 2004.

Cette diminution d'une année à l'autre s'explique en partie par le processus simplifié d'acceptation des plaintes mis en place en 2007. Selon ce processus, lorsqu'une personne formule une plainte qui est, dans les faits, similaire à d'autres plaintes déjà sous enquête, nous informons cette personne que la question est déjà sous enquête et sera prise en compte par la commissaire dans ses conclusions. Cette approche est également utilisée dans le cas des plaintes pour lesquelles nous avons déjà tiré des conclusions dans une cause similaire.

Dans de tels cas, nous offrons aux plaignants la possibilité d'invoquer des conclusions similaires afin de résoudre les problèmes particuliers qu'ils peuvent avoir avec une organisation.

Par exemple, nous poursuivons présentement cinq enquêtes concernant le dépistage des drogues dans le cadre d'un emploi. Dans les circonstances, 27 autres personnes ont accepté de ne pas déposer de plainte officielle ayant trait au même enjeu.

Dans certains cas, bien que la situation d'une personne soit similaire à celle d'une autre qui a porté plainte, les faits peuvent être suffisamment différents pour justifier une enquête complète.

Une autre cause possible de la baisse du nombre de plaintes est que les organisations connaissent peut-être mieux leurs obligations liées à la protection de la vie privée. De plus, bon nombre d'entre elles disposent maintenant de processus internes de résolution des plaintes afin de régler avec leurs clients les questions de protection de la vie privée. La Section des demandes de renseignements conseille également aux gens de chercher à régler leurs différends avec les organisations avant de déposer une plainte officielle au Commissariat.

# ENQUÊTES SUR LES PLAINTES ET DEMANDES DE RENSEIGNEMENTS

Les Canadiennes et Canadiens étant davantage au fait des enjeux relatifs à la protection de la vie privée, les organisations doivent faire en sorte de s'acquitter de leurs responsabilités concernant les renseignements personnels. De façon plus particulière, les consommateurs connaissent de mieux en mieux les graves ramifications du vol d'identité, ce qui les amène à insister davantage auprès des entreprises pour qu'elles respectent leurs obligations lorsqu'elles recueillent des renseignements personnels.

Les gens ne souhaitent pas que de l'information de nature délicate telle que leur numéro de permis de conduire soit recueillie et conservée sans raison légitime, tout comme ils ne veulent pas que le numéro de leurs cartes de crédit et les dates d'expiration soient imprimés sur les reçus.

Bon nombre d'entreprises prennent au sérieux leurs responsabilités en matière de protection de la vie privée. Par contre, il ne fait pas de doute – d'après les plaintes reçues et les atteintes à la sécurité des données volontairement déclarées au Commissariat – qu'une grande quantité d'organisations pourraient en faire davantage.

Les entreprises qui manipulent les renseignements personnels doivent régulièrement mettre à jour leurs politiques et pratiques en matière de protection de la vie privée. Elles doivent tenir à jour leur système de sécurité des données. De plus, il leur faut veiller à ce que les employés soient informés des changements et reçoivent une formation régulière.

## Demandes de renseignements

La Section des demandes de renseignements répond aux questions des Canadiennes et Canadiens, des institutions gouvernementales, des organisations du secteur privé et du milieu juridique. Les agents responsables des demandes de renseignements fournissent de l'information sur un vaste éventail d'enjeux en vertu de la *LPDP* et de la *Loi sur la protection des renseignements personnels*.

d'un code relatif aux employés reposant sur le critère des fins raisonnables, en combinaison avec la notion du Code civil du Québec qui oblige les employeurs à respecter la dignité des travailleurs.

- Nous avons demandé davantage de latitude pour refuser et/ou abandonner des plaintes si leur enquête ne répond à aucun but utile ou ne sert pas l'intérêt public, ce qui nous permettrait alors de concentrer nos ressources d'enquête sur des questions d'un intérêt systémique plus vaste.

La date limite pour faire parvenir des observations à Industrie Canada était la mi-janvier 2008. Le ministère a reçu 67 mémoires et en faisait l'examen au début de 2008. Nous sommes impatientes de passer à la prochaine étape de l'examen de la Loi et à l'important dialogue qu'il engendra entre les défenseurs du droit à la vie privée, les organes de réglementation, l'industrie et les parlementaires.

Le gouvernement du Canada a déposé sa réponse en octobre. Selon nous, l'un des éléments très importants de la réponse concernait la reconnaissance du fait que les menaces à la protection de la vie privée font de plus en plus appel à des mesures d'envergure internationale. L'industrie du traitement des données s'internationalise toujours plus, tout comme le font les risques posés à la sécurité des données.

La coopération intergouvernementale, le partage de renseignements entre les administrations et l'attention accordée aux tendances qui se dessinent dans d'autres parties du monde sont tous devenus des considérations stratégiques cruciales alors que nous travaillons à protéger la vie privée des Canadiennes et Canadiens.

En octobre, Industrie Canada a présenté un avis de consultation pour obtenir l'opinion du public quant à la meilleure manière de mettre en œuvre certaines dispositions de la réponse gouvernementale. On a accordé une importance particulière aux points de vue sur les dispositions relatives à la notification des atteintes à la sécurité des données, et aux concepts de « produit du travail » et d'« autorité légitime ». En outre, Industrie Canada a cherché à obtenir des opinions sur les déclarations des témoins, le consentement des mineurs et les organismes d'enquête.

Dans le cadre de cette série de consultations, la commissaire à la protection de la vie privée a demandé au ministre de l'Industrie d'examiner étroitement cinq enjeux qui auront une incidence marquée sur notre travail dans les années à venir :

- Nous avons continué de promouvoir une approche « contextuelle » en ce qui touche l'information sur le produit du travail.
- Nous avons plaidé en faveur d'une notification obligatoire des atteintes à la sécurité des données, et insisté sur la nécessité d'établir clairement des déclencheurs et des seuils dans toute nouvelle disposition de la LPPDE.
- Nous avons demandé à ce que demeurent ouvertes les modifications possibles à la LPPDE concernant l'accès aux documents visés par le secret professionnel qui lie un avocat à son client, en attendant une décision de la Cour suprême du Canada dans l'affaire de la Commissaire à la protection de la vie privée du Canada c. Blood Tribe Department of Health.

- Nous avons insisté pour que toute nouvelle disposition sur la protection de la vie privée dans le contexte de la relation employeur-employé prenne en considération les lois de l'Alberta et du Québec afin de mieux reconnaître le fait que l'inégalité du pouvoir de négociation dans les relations de travail implique que les employés pourraient ne pas se sentir en position de refuser de consentir à la collecte de leurs renseignements personnels. Le CPVP voit l'avantage de l'approche albertaine

Heureusement, les concepteurs de la *LPRPDE* ont reconnu l'importance de procéder à des mises à jour régulières. Ainsi, le Parlement est tenu de réviser tous les cinq ans la partie de cette loi qui porte sur la protection des données.

Le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes a pris en charge le premier travail de révision quinquennale. Ses activités en ce sens ont débuté durant l'été 2006. En février 2007, les membres du Comité ont conclu les audiences publiques qui ont porté sur un éventail d'enjeux. Ils ont entendu 67 témoins et pris en considération 34 mémoires de la part de particuliers, d'associations du secteur privé, de défenseurs du droit à la vie privée et de la commissaire à la protection de la vie privée.

Dans l'ensemble, nous avons le sentiment que la Loi a été bien accueillie, quelle fonctionne raisonnablement bien et que nous disposons de la plupart des outils et des pouvoirs voulus pour la faire appliquer. La Loi offre à la population canadienne de solides protections de la vie privée dans la sphère commerciale.

Dans nos présentations au Comité, nous avons indiqué que la loi n'est pleinement en vigueur que depuis 2004. Bien que l'expérience acquise à ce jour ait été instructive, il faut plus de temps avant que ne surviennent des changements d'envergure et que ne se fassent sentir toutes les répercussions d'une loi complexe.

Cela dit, certains ajustements seraient souhaitables pour s'assurer que les mesures de protection de la vie privée évoluent au même rythme que les nouvelles tendances et technologies.

En mai 2007, le Comité a présenté son rapport final, qui incluait 25 recommandations aux fins d'examen par le gouvernement ou de discussions.

Les modifications suggérées touchaient un grand nombre d'enjeux, dont les suivants : renseignements sur les personnes-ressources du monde des affaires; renseignements sur le produit du travail, tels que les habitudes de prescription des médecins; relations employé-employeur; organismes d'enquête; déclarations des témoins; application de la loi et sécurité nationale; exceptions pour la personne ou la famille; communication des renseignements personnels avant le transfert d'entreprises; mesures de protection supplémentaires pour les mineurs; notification obligatoire des atteintes à la sécurité des données.

Nous sommes profondément reconnaissants des efforts des parlementaires, chercheurs, organisations et citoyens qui ont mis leur expérience et leurs compétences au profit du processus d'examen.



# AMÉLIORATION DE LA LPRPDE : UN EXAMEN DE NOTRE LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS À L'INTENTION DU SECTEUR PRIVÉ

Un comité parlementaire a réalisé un examen obligatoire de la LPRPDE en 2007 – une étape importante pour raffermir les mesures de protection de la vie privée des Canadiennes et Canadiens

La LPRPDE, ainsi que son pendant pour le secteur public, la *Loi sur la protection des renseignements personnels*, de même que les lois provinciales relatives à la protection de la vie privée, fournissent l'assise de la protection de la vie privée au Canada.

Le paysage de la protection de la vie privée change constamment – et nos lois doivent suivre le rythme.

On n'a qu'à songer à la profondeur des changements survenus dans le monde depuis dix ans, alors que nous commençons à parler de ce à quoi devrait ressembler une loi sur la protection de la vie privée dans le secteur privé au Canada.

À l'époque, le terme « inforoute » se voulait accrocheur. Aujourd'hui, c'est une réalité. Le mince filet de renseignements personnels traversant les frontières s'est transformé en torrent. Dans l'intervalle, de nouvelles technologies telles que les dispositifs de repérage soumettent la protection de la vie privée à de nouveaux périls. Et les conséquences du 11 septembre font en sorte que les gouvernements demandent aux entreprises davantage de renseignements sur nos vies au quotidien.

Il est crucial que la LPRPDE puisse continuer à répondre à tous ces nouveaux défis. La *Loi sur la protection des renseignements personnels*, qui est désespérément dépassée – elle n'a pas changé en 25 ans – est la preuve qu'il est dangereux de négliger de moderniser les lois sur la protection des renseignements personnels.



## Manière dont le Commissariat aide les organisations à prévenir les atteintes à la sécurité des données

- Nous avons lancé un outil d'apprentissage en ligne qui offre aux détaillants un guide contenant les étapes à suivre pour protéger les renseignements personnels des clients et répondre aux obligations de la LPPDE.
- Nous avons publié divers documents électroniques et imprimés sur la manière dont les entreprises peuvent sauvegarder des renseignements personnels, y compris la brochure intitulée « Protection des renseignements personnels : vos responsabilités – Guide à l'intention des entreprises et des organisations ».
- De concert avec des groupes industriels et des groupes de défense des consommateurs, nous avons élaboré des lignes directrices d'application volontaire concernant les atteintes à la sécurité des données.
- Nous conseillons et épaulons les organisations qui prennent des mesures en réaction à des atteintes à la sécurité des données, notamment en donnant des conseils sur les notifications à fournir aux personnes touchées par ce problème.
- Nous continuons à faire pression sur le gouvernement fédéral pour qu'il rende obligatoire les notifications d'atteintes à la sécurité des données en vertu de la LPPDE, ce qui, selon nous, encouragerait les entreprises à améliorer leurs mesures de sécurité.
- Nous vérifions la façon dont les organisations visées par la LPPDE gèrent les renseignements personnels lorsque nous avons des motifs raisonnables de croire qu'une organisation enfreint la loi.
- Nos enquêtes sur les plaintes concernant la vie privée aident à cerner les mesures que peuvent prendre les entreprises pour mieux protéger les renseignements personnels.

## PRÉPARER L'AVENIR

La société TJX s'est conformée à toutes les recommandations du CPVP visant à améliorer la sécurité, le contrôle et d'autres enjeux entourant la gestion des renseignements personnels.

Un an après qu'on l'a mise au jour, la fuite engendre encore des répercussions.

L'entreprise continue de répondre à certaines poursuites engagées contre elle. La Federal Trade Commission des États-Unis poursuit son enquête à l'instar du secrétaire à la Justice du Massachusetts au nom d'un groupe de plus de 30 secrétaires à la Justice d'États.

On ignore combien la fuite coûtera ultimement à l'entreprise – mais le total se chiffrera certainement en centaines de millions de dollars.

Avant la fin de 2007, TJX avait désigné un chef de la protection des renseignements personnels et recherchait un directeur de la protection de la vie privée pour élaborer et mettre en œuvre un programme complet de sécurité et de protection de la confidentialité des renseignements personnels.

## DE LOURDES DÉFAILLANCES

L'enquête a mis en lumière quelques défaillances critiques :

1. TJX recueillait trop de renseignements et les conservait beaucoup trop longtemps.

L'entreprise n'aurait pas dû recueillir les numéros de permis de conduire et autres numéros d'identification lors des retours de marchandises sans reçu. Un permis de conduire est la preuve qu'une personne est autorisée à conduire une auto – non pas un identificateur servant à analyser les habitudes concernant les retours de marchandises. En outre, un numéro de permis de conduire est inutile pour identifier des voleurs.

En réponse à nos préoccupations, TJX a proposé un nouveau processus novateur pour prévenir les retours de marchandises frauduleux. L'entreprise continuera de recueillir et introduire dans le système de terminaux des points de vente des renseignements tels que le numéro du permis de conduire. Toutefois, le numéro sera instantanément converti en un numéro d'identification unique, permettant ainsi de faire le suivi des retours de marchandises non accompagnée d'un reçu sans conserver les numéros d'identification originaux.

Avant l'affaire de l'accès non autorisé, les renseignements d'identification recueillis auprès des personnes rapportant de la marchandise étaient conservés indéfiniment.

L'entreprise conservait également pendant longtemps les données relatives aux cartes de crédit. En fait, certains des renseignements volés impliquaient des transactions qui remontaient à plusieurs années.

2. TJX a négligé de mettre à jour en temps opportun ses systèmes de sécurité.

Il a fallu deux années à TJX pour réaliser une conversion vers un protocole cryptographique à jour. C'est durant cette période que se sont produites les atteintes à la sécurité des données. Par conséquent, l'entreprise n'a pas respecté les exigences en matière de normes de sécurité des données décrites par l'industrie des cartes de paiement.

3. TJX n'a pas surveillé adéquatement son système, ce qui l'a empêchée de déceler les signes d'une intrusion.

Les voleurs ont été en mesure de poursuivre le vol de données pendant une année et demie avant que TJX n'apprenne la présence de logiciels douteux dans une partie de son système informatique. En appliquant des mesures de contrôle adéquates, TJX aurait découvert cet incident plus tôt.



## ENQUÊTE SUR UNE ATTEINTE À LA SÉCURITÉ DES DONNÉES

### L'AFFAIRE TJX : COMMENT DES PIRATES ONT PU ACCÉDER À 94 MILLIONS DE CARTES DE CRÉDIT ET DE DÉBIT

Ce qu'on a décrit comme étant le plus grand vol en ligne jamais réalisé a commencé un jour d'été de 2005.

On croit que les voleurs, armés d'une antenne, d'un ordinateur portatif et de quelques logiciels spécialisés, se sont retrouvés à l'extérieur d'un magasin Marshalls à Miami et ont fait irruption dans les réseaux locaux sans fil et faiblement protégés du magasin.

Une fois à l'intérieur, ils ont utilisé les serveurs informatiques qui traitent et stockent les renseignements sur les clients obtenus lors de transactions effectuées pour des centaines de magasins appartenant à TJX, ce géant de la vente au détail à marge réduite, y compris Winners et HomeSense au Canada.

Pendant un an et demi, les voleurs ont pillé le système informatique de TJX.

Au bout du compte, ils auront accédé à au moins 94 millions de cartes de crédit et de débit ainsi qu'aux noms, adresses et numéros de permis de conduire de gens qui avaient rapporté de la marchandise dans les magasins de TJX.

Il ne s'agissait pas d'un crime particulièrement compliqué. On trouve facilement sur Internet des instructions détaillées sur la manière de déchiffrer le protocole cryptographique servant à protéger les réseaux sans fil de TJX.

C'est un fait bien établi depuis un certain temps que ce protocole cryptographique — le système WEP (Wired Equivalent Privacy, ce qui signifie confidentialité équivalente aux transmissions par fil) — ne protégeait pas adéquatement le réseau puisqu'une personne possédant un peu de savoir-faire en informatique pouvait facilement le contourner.

TJX était au fait des préoccupations entourant son protocole cryptographique et était en voie de se convertir à une technologie plus fiable au moment où est survenu l'accès non autorisé. Selon nous, la conversion ne s'est pas faite dans un délai raisonnable.

L'enquête du CPVP, réalisée de concert avec le commissaire à l'information et à la protection de la vie privée de l'Alberta, Frank Work, a mené à la conclusion que TJX ne s'était pas conformée aux lois fédérales et albertaines sur la protection des renseignements personnels.

Plus des trois quarts des Canadiennes et Canadiens (77 p. 100) croient qu'il faudrait avertir les organismes gouvernementaux et les personnes touchées lorsque des renseignements personnels délicats sont compromis par suite d'une atteinte à la sécurité des données, selon un sondage commandé en 2007 par le Commissariat. Entre-temps, 66 p. 100 souhaitaient être avisés dans le cas de compromission de renseignements non délicats.

Selon un des principes de la *LPRPD*, les gens devraient avoir prise sur leurs renseignements personnels. La notification des atteintes à la sécurité des données donne un choix aux gens. Ainsi, ils peuvent décider par eux-mêmes de la manière de réagir à une telle atteinte, en décidant par exemple que ce serait une bonne idée de vérifier plus souvent leurs rapports de crédit, ou encore qu'aucune mesure n'est justifiée.

Ce qui compte, c'est que la personne ait prise sur ses renseignements personnels.

Le Commissariat croit que l'envoi d'une notification est un élément important d'une approche globale pour réduire les atteintes à la sécurité des données.

La débacle de TJX, en plus des manchettes concernant les disques informatiques et disques durs manquants ainsi que d'autres données perdues, constitue un avertissement pour toutes les organisations qui recueillent des renseignements personnels. Ces incidents illustrent de façon frappante à quel point il est important que les entreprises accordent la priorité à la protection de la vie privée et à la sécurité.

Lorsque les Canadiennes et Canadiens confient leurs renseignements personnels à une organisation, ils s'attendent à ce que ces renseignements soient bien protégés – ce que la loi exige d'ailleurs.

À titre d'exemple, le vol d'ordinateur portatif est un type courant d'atteinte à la sécurité des données. Des employés quittent le bureau avec des ordinateurs portatifs contenant des renseignements personnels délicats sur les clients — ce qui est contraire aux politiques de l'entreprise en matière de sécurité.

L'efficacité des politiques et des procédures dépend de la qualité de la formation qui vise à raffermir leur application.

Malheureusement, un sondage mené en 2007 auprès des entreprises canadiennes pour le Commissariat a révélé que seulement le tiers d'entre elles avaient formé leur personnel à l'égard de leurs responsabilités découlant des lois canadiennes en matière de protection des renseignements personnels. Les grandes entreprises étaient les plus susceptibles d'avoir offert une formation, comme l'indiquaient 63 p. 100 d'entre elles.

Les entreprises n'ayant donné aucune formation aux employés qui gèrent les renseignements personnels s'exposent à des risques beaucoup plus grands d'atteinte à la sécurité des données. Nous espérons que les résultats seront plus encourageants la prochaine fois que nous mènerons un sondage sur la conformité à la *LPRPDE*.

Au cours de 2007, nous avons élaboré des directives concernant les atteintes à la sécurité des données, en consultation avec l'industrie et des groupes de la société civile. Ces directives énoncent les principales étapes que devraient suivre les organisations victimes d'un accès non autorisé, comme contenir l'atteinte, évaluer les risques connexes, informer les personnes touchées et prévenir les fuites futures. La Nouvelle-Zélande a également adopté ces directives comme modèle à suivre et la commissaire à la protection de la vie privée de l'Australie se propose de faire de même.

Nous avons clairement indiqué que les directives facultatives n'éliminaient pas la nécessité d'avoir une loi prévoyant la notification des atteintes à la sécurité des données. En fait, nous avons exhorté le gouvernement fédéral à modifier la *LPRPDE* afin d'y ajouter une disposition sur la notification des atteintes à la sécurité des données.

Nous sommes d'avis qu'une notification obligatoire aiderait à protéger les renseignements personnels de deux manières très importantes. Premièrement, cela encouragerait les organisations à prendre plus au sérieux la protection de la vie privée et la sécurité. Deuxièmement, les gens disposeraient de l'information voulue pour prendre des mesures afin de se protéger eux-mêmes contre le vol d'identité ou d'autres formes de fraude.

Il ne fait pas de doute que les gens désirent ce genre d'information.

L'évocation du nom « TJX » est sans aucun doute très convaincante lorsque des experts en matière de sécurité demandent aux cadres supérieurs des fonds pour mettre à niveau le système de sécurité.

Toutes les organisations doivent recourir à un système de sécurité solide pour protéger les renseignements personnels. Dire en guise d'excuse que « Nous n'étions pas plus lents que les autres compagnies » ne suffit pas.

Les mesures de sécurité efficaces coûtent cher, mais beaucoup moins que la réparation des dégâts par suite d'une fuite de données majeure. Selon les experts en matière de sécurité, les atteintes importantes à la sécurité des données coûtent plusieurs fois le coût de l'installation de sauvegardes adéquates dès le départ.

De bonnes pratiques en matière de protection de la vie privée sont également très efficaces pour protéger les renseignements personnels.

La *LPRPD* énonce dix principes relatifs à l'équité dans le traitement des renseignements que doivent suivre les entreprises. Ces principes – parfois appelés « règles d'or » de la protection de la vie privée – incluent des éléments fondamentaux tels que l'obtention du consentement pour l'utilisation des renseignements personnels; la limitation de l'utilisation, de la communication et de la conservation des renseignements personnels; et l'utilisation de mesures de sécurité appropriées.

Le point de départ de la mise en œuvre de ces principes est l'examen objectif des renseignements personnels recueillis. Les organisations ne devraient recueillir que les renseignements personnels absolument essentiels. Après tout, si vous ne disposez pas de ce type d'information, vous ne pouvez le perdre ou vous le faire voler.

La seconde étape cruciale consiste à reconnaître la valeur des renseignements personnels recueillis et à les protéger adéquatement.

En suivant ce conseil de base, une organisation devrait se retrouver avec un objectif de collecte des données relativement petit et bien protégé.

Le CPVP a élaboré une formation en ligne plus détaillée sur la manière dont les détaillants peuvent mettre en pratique les principes relatifs à l'équité dans le traitement des renseignements personnels. Le cours est offert sur notre site Web.

La formation des employés est également cruciale pour prévenir les fuites de données. Dans bon nombre de rapports que nous avons reçus des entreprises, la cause de l'atteinte à la sécurité des données était le défaut d'un employé de respecter les procédures de la compagnie.

La taille de la pire atteinte à la sécurité des données survenue en 2007 est ahurissante. L'intrusion dans le système informatique de TJX a touché quelque 94 millions de numéros de cartes de débit et de crédit appartenant à des gens de plusieurs pays — c'est la plus grande atteinte à la protection des renseignements personnels jamais consignée.

Dans un cas survenu au Royaume-Uni, un responsable du ministère des revenus et douanes de Sa Majesté n'a pas tenu compte des procédures de sécurité, et a inséré dans une enveloppe deux disques contenant les détails personnels de 25 millions de bénéficiaires de prestations pour enfants. L'enveloppe a alors été postée par le biais d'un système de courrier interne. Les disques ne se sont pas rendus chez le destinataire, qui se trouvait dans un autre ministère.

Ici au Canada, un disque dur appartenant à une filiale de la CIBC a disparu — ainsi que les renseignements personnels de près d'un demi-million de clients.

Bien entendu, les données compromises dans ce type de fuites ne se retrouvent pas toutes entre les mains de criminels.

Toutefois, il ne fait pas de doute que les escrocs ont vu dans les données personnelles une mine d'or. Le vol d'identité est endémique — et lucratif.

Les entreprises reconnaissent la valeur des

renseignements personnels en ce qui les concerne — dans le cas des campagnes de marketing ciblées, par exemple. Malheureusement, cette perception ne se traduit pas toujours en mesures de sécurité aptes à protéger les renseignements de la main des criminels.

Ainsi, peu avant que la fuite de TJX ne devienne publique, Visa USA a révélé qu'un peu plus du tiers des plus grands détaillants dans ce pays se conformaient à la norme de sécurité de l'industrie. Le chiffre concernant d'autres importants marchands était encore pire — seulement 15 p. 100.

Nous retenons que la situation aux États-Unis comme au Canada s'est améliorée dans le sillage de l'affaire TJX. Visa Canada nous a appris que pratiquement tous les grands détaillants étaient tout près de la conformité à la norme de sécurité des données établie pour les sociétés émettrices de cartes de paiement.

NOTE : L'information sur les atteintes à la sécurité des données qui ont été spontanément déclarées au Commissariat en 2007 se trouve à la page 44.



## ENJEU CLÉ : ATTEINTES À LA SÉCURITÉ DES DONNÉES

### Jouer avec des renseignements personnels

*En 2007, de nombreux désastres ont eu lieu sur le plan de la confidentialité des données, mettant en lumière la nécessité que les entreprises reconnaissent la valeur des renseignements personnels et s'efforcent davantage de les protéger*

Il n'y a pas si longtemps, un groupe de cadres supérieurs débattaient du bien-fondé de retarder la mise à niveau du système de sécurité informatique désuet de leur entreprise. L'un d'entre eux a mis en garde ses collègues dans un courriel :

*« Il faut que nous soyons prêts à courir ce risque dans le souci d'économiser tout en souhaitant ne pas nous compromettre. » [Traduction]*

Ces mots étaient prémonitoires.

Ils ont été écrits par un vice-président de TJX – un nom devenu synonyme d'atteinte à la sécurité des données. Le courriel a été rendu public durant le procès contre TJX.

En fait, les pirates informatiques avaient déjà fait effraction dans le système informatique du détaillant international à marge réduite et étaient occupés à chaparder les renseignements personnels de gens qui magasinait chez Winners, HomeSense et d'autres magasins appartenant à TJX. La technologie obsolète de chiffrement de la compagnie ne suffisait pas à protéger ces données délicates.

TJX était l'une des nombreuses entreprises jouant à la roulette russe avec les renseignements personnels des Canadiennes et Canadiens.

Les grandes entreprises sous-estiment trop souvent la valeur des renseignements personnels et le risque qu'ils deviennent la cible des voleurs. Par conséquent, nous constatons des sauvegardes déficientes, des politiques et procédures nonchalantes en matière de sécurité et de protection de la vie privée – et, bien sûr, des fuites de données.



et de mettre à jour des normes et des lignes directrices pour traiter des aspects liés à la sécurité de la gestion de l'identité, à la biométrie et à la protection des données personnelles.

- Participation aux activités de l'International Working Group on Data Protection in Telecommunications, qui s'est récemment concentré sur la protection de la vie privée sur Internet.
- Rôle de premier plan dans la création d'une association internationale d'autorités de protection des données et d'autres agences d'application de la loi d'États francophones.
- Membre du Forum des autorités de protection de la vie privée de la zone Asie-Pacifique.

## Autres faits saillants

- Préparation d'un mémoire et comparution devant la Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India.
- Versement de subventions de recherche à huit organisations par le biais de notre programme des contributions – portant à plus de 1 million de dollars le financement total fourni ces quatre dernières années pour des projets de recherche sur la protection de la vie privée.

- Coanimation, de concert avec le groupe de droit et de technologie de l'Université d'Ottawa, d'un Symposium sur la protection de la vie privée sur Internet pour examiner les nouvelles menaces à la vie privée en ligne, les nouvelles tendances et les façons de mieux protéger les renseignements personnels dans l'avenir.

- Animation en février 2007 à Winnipeg d'une conférence pour les enquêteurs. 56 enquêteurs du CPVP et 11 enquêteurs de bureaux provinciaux et territoriaux ont assisté à la conférence.

- Comparution dans de nombreuses affaires judiciaires afin d'aider à développer une jurisprudence qui tienne compte de la protection de la vie privée au Canada.

## Appui aux entreprises

- Lancement d'un outil d'apprentissage électronique pour aider les détaillants à s'assurer que leurs pratiques et politiques en matière de protection de la vie privée sont conformes à leurs obligations juridiques et qu'ils fournissent à leur clientèle les mesures de protection de la vie privée garanties en vertu de la *LPDP*.
- Publication de lignes directrices pour aider les organisations à prendre les bonnes mesures après une atteinte à la vie privée, y compris l'envoi d'avis aux gens qui risquent de subir des inconvénients en raison du vol, de la perte ou de la communication par erreur de leurs renseignements.
- Amorce d'un programme de liaison régionale pour étendre aux petites et moyennes entreprises les efforts de sensibilisation en matière de conformité et y apporter les adaptations nécessaires.

## Initiatives mondiales

- Animation de la Conférence internationale des commissaires à la protection des données et de la vie privée — la plus importante jamais tenue du genre — pour honorer une promesse faite en 2002.
- Présidence d'un groupe de l'OCDE chargé d'améliorer la coopération entre les autorités de protection des données et d'autres organismes chargés de l'application du droit à la protection de la vie privée partout dans le monde. L'OCDE a adopté une recommandation sur la coopération transfrontalière fondée sur le travail du groupe de bénévoles.
- Participation aux efforts d'un groupe de l'APEC s'intéressant à la confidentialité des données pour mettre en œuvre un nouveau cadre de protection de la vie privée pour les pays membres de l'APEC.
- Travail de concert avec le Conseil canadien des normes à l'élaboration de normes internationales en matière de protection de la vie privée.
- Participation aux activités de l'Organisation internationale de normalisation (ISO); membre d'un important groupe de travail ISO responsable d'élaborer

Soutien proactif du Parlement

- Comparution devant des comités parlementaires sur des questions telles que le vol d'identité et des modifications à la *Loi électorale du Canada*.
- Travail de concert avec le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique sur l'examen de la *LPRPDE* prévu par la Loi; réponse à une consultation d'Industrie Canada sur l'examen de la *LPRPDE*.
- Travail conjoint avec des homologues provinciaux et territoriaux pour l'adoption d'une résolution exhortant le gouvernement fédéral à suspendre son nouveau programme visant à faire paraître une liste de personnes interdites de vol d'ici à ce qu'on puisse le réviser pour s'assurer de la protection rigoureuse de la vie privée des Canadiennes et Canadiens.

Au service de la population canadienne

- Réponse à plus de 7 500 demandes de renseignements liées à la *LPRPDE*.
- Enquête sur des centaines de plaintes concernant la vie privée dans les secteurs public et privé.
- Création d'un blogue pour aider à développer des liens et à stimuler la discussion sur des questions d'intérêt pour les Canadiennes et Canadiens en ce qui touche la protection de la vie privée.
- Amorce du travail sur une campagne de marketing social visant à promouvoir la sensibilisation et à agir pour la protection de la vie privée des enfants en ligne.





détails personnels. Nous sommes à élaborer des outils qui aideront les gens à gérer leur identité en ligne.

## Sécurité nationale

Les mesures de sécurité nationale adoptées dans le sillage des attaques survenues le 11 septembre 2001 ont transformé le paysage de la protection de la vie privée au Canada et dans le monde.

Il est arrivé trop souvent que ces mesures portent sur la collecte et le partage de renseignements personnels sans beaucoup de surveillance et de considération à l'égard de la vie privée et d'autres droits individuels. Une liste croissante d'organisations du secteur privé – transporteurs aériens, banques et cabinets comptables, par exemple – ont été mises à contribution pour recueillir des renseignements personnels pour l'État.

La façon dont nous abordons la sécurité doit témoigner des valeurs fondamentales de notre société – y compris le droit à la protection de la vie privée. Nous devons constamment nous demander pourquoi nous acceptons le glissement continu vers la sécurité au détriment de la protection de la vie privée. Est-ce toujours justifié? Est-ce irréversible?

Ce sont les messages que nous continuerons de répéter dans le cadre de notre travail pour nous assurer que les initiatives axées sur la sécurité nationale protègent adéquatement la vie privée.

## Information génétique

Les progrès en génétique engendrent un éventail de défis nouveaux et complexes pour la protection de la vie privée.

L'intérêt envers l'obtention de données d'ordre génétique s'accroît rapidement. Le dépistage génétique à des fins d'emploi, d'affaires criminelles, de recherche, de soins médicaux, d'accès à une assurance ainsi que pour déterminer les liens de parenté soulève dans tous les cas d'importantes et très délicates questions en matière de protection de la vie privée.

Il est nécessaire de sensibiliser davantage le public à l'usage qu'on peut faire de l'information génétique. Nous devons également examiner certains des nouveaux défis qui se posent à la protection de la vie privée dans un monde où nos gènes en révèlent si long à notre propos.

En 2007, nous avons démontré que le Commissariat peut améliorer la situation dans ce domaine après avoir mis au jour des préoccupations liées à la protection de la vie privée découlant de l'intégration de photographies prises dans la rue avec une technologie de cartographie fondée sur le Web. Ce type de photographie implique l'utilisation de caméras vidéo à haute résolution, souvent apposées à des véhicules qui circulent dans les rues de la ville. Ces images — notamment celles de gens qu'on peut identifier — sont alors affichées sur Internet.

C'est devenu un genre de sport cybernétique que de trouver des photos de gens surpris dans des situations embarrassantes ou personnelles — comme un homme qui sort d'un magasin de vidéocassettes pour adultes ou une jeune femme en train de se faire bronzer — et de les diffuser sur le Web.

« Street View », de Google, est l'un des services mis en place. À ce jour, Street View a produit des photographies prises dans des villes américaines. Nous craignons que les photographies prises dans la rue, comme la chose se produit actuellement aux États-Unis, ne répondent pas aux exigences de base des lois sur la protection de la vie privée ici au Canada. J'ai écrit à Google pour exposer ces préoccupations, et des responsables de cette compagnie nous ont donné l'assurance qu'ils veilleront à ce que Street View soit conforme aux lois canadiennes s'il est offert au Canada.

## Gestion de l'identité

L'enjeu lié à l'intégrité et à la protection de l'identité découle du fait que des quantités massives de données circulent sans arrêt.

Les renseignements personnels sont devenus un produit recherché, non seulement par des organisations légitimes, mais par des criminels également. Nous avons assisté à une véritable explosion de vols d'identité ces dernières années — un crime qui comporte des coûts à la fois économiques et émotifs.

L'amélioration des pratiques de gestion des renseignements personnels peut considérablement réduire la possibilité que les données se retrouvent entre les mains de voleurs d'identité. Notre objectif est de sensibiliser davantage le public à l'importance de manipuler les renseignements personnels avec le plus grand soin. Nos efforts d'éducation publique viseront les organisations comme les particuliers.

Nous accorderons une grande importance au monde en ligne, alors que les renseignements personnels se propagent de plus en plus sur les sites commerciaux, les réseaux sociaux et les blogs personnels. Les gens découvrent que les renseignements personnels qu'ils ont affichés sont utilisés d'une manière qu'ils n'avaient pas imaginée. Dans certains cas, des imposteurs dérobent un profil au complet — nom, photo et autres

L'univers sans cesse changeant des enjeux relatifs à la protection de la vie privée signifie que le Commissariat doit trouver des moyens de concentrer ses efforts. En 2007, nous avons défini quatre nouvelles priorités stratégiques qui, croyons-nous, représentent certaines des plus lourdes menaces posées à la protection de la vie privée des Canadiennes et Canadiens.

Ces priorités – technologie de l'information, gestion de l'identité, sécurité nationale et information génétique – nous aideront à orienter notre travail en matière de politique, de recherche et d'enquête au cours des trois prochaines années.

## Technologie de l'information

La technologie de l'information (TI) était un choix évident à retenir pour notre liste étant donné que pratiquement chaque question que nous traitons en matière de protection de la vie privée et pratiquement chaque plainte que nous recevons concernant protection de la vie privée comporte un élément de TI.

Les technologies de l'information et des communications font dorénavant partie intégrante de notre quotidien. Les progrès technologiques signifient que de plus en plus de renseignements personnels peuvent être recueillis, stockés, analysés et éventuellement accessibles de partout dans le monde.

Ces développements apportent des avantages incontestables sur le plan de l'utilité et de l'efficacité, mais ils posent également des risques énormes à la protection de la vie privée. Les gouvernements et les entreprises peuvent maintenant recueillir et utiliser des données personnelles dans une mesure qu'on ne pouvait même pas imaginer jusqu'à tout récemment.

Le Commissariat continuera de développer ses capacités d'évaluer l'incidence sur la vie privée des nouvelles technologies. Nous chercherons également à aider les Canadiennes et Canadiens à comprendre et, dans la mesure du possible, à atténuer cette incidence.





# LA PROTECTION DE LA VIE PRIVÉE EN CHIFFRES EN 2007

538	Nombre mensuel moyen de demandes de renseignements liées à la LRPPE :
28	Nombre mensuel moyen de plaintes liées à la LRPPE :
33	Nombre mensuel moyen d'enquêtes fermées dans le cadre de la LRPPE :
420	Total d'enquêtes fermées durant l'année :
7	Comparutions devant le Parlement :
15	Nombre de lois/projets de loi examinés pour en dégager les répercussions sur la protection de la vie privée :
19	Activités de recherche commandées :
92	Allocutions et présentations données :
474	Demandes des médias :
301	Interviews données :
44	Communiqués de presse émis :
2 043	Publications distribuées :
39 429	Nombre mensuel moyen de visites du Canada sur notre site Web :
86 155	Nombre mensuel moyen de visites d'autres pays sur notre site Web :
14 173	Nombre mensuel moyen de visites sur notre blogue :
82	Avis juridiques préparés :
3	Décisions rendues dans le cadre du règlement de litiges aux termes de la LRPPE :
5	Litiges réglés :
21	Demandes reçues et menées à terme en vertu de la Loi sur l'accès à l'information entre avril 2007, alors que nous étions assujettis à cette loi pour la première fois, et la fin de l'année civile (toutes gérées dans les délais prescrits) :
14	Demandes reçues et menées à terme pendant la même période en vertu de la Loi sur la protection des renseignements personnels :



## Bienvenue à la commissaire adjointe

Je suis grandement enchantée de l'arrivée d'Elizabeth Denham, notre nouvelle commissaire adjointe à la protection de la vie privée, qui nous aidera à diriger la recherche de solutions novatrices aux importants défis qui se poseront au Canada dans les années à venir en matière de protection de la vie privée.

Avant sa nomination, Mme Denham était à la tête de la Direction de la recherche, de l'analyse et des relations avec les intervenants du Commissariat. Elle occupait auparavant le poste de directrice, Secteur privé au Commissariat à l'accès à l'information et à la protection de la vie privée de l'Alberta.

Il ne fait aucun doute que l'expérience de Mme Denham dans le développement de relations avec les intervenants, la perspective qu'elle s'est forgée par le biais de son travail avec les commissaires provinciaux et ses vastes compétences spécialisées dans le domaine de la protection de la vie privée seront extrêmement profitables pour le Commissariat dans les années à venir. Elle veillera à l'application de la *LPDP* aux côtés de Raymond D'Aoust, commissaire adjoint responsable de la *Loi sur la protection des renseignements personnels*.

## Une équipe consciencieuse et experte en la matière

J'aimerais souligner le travail très intense réalisé l'année dernière par la consciencieuse équipe du Commissariat. L'animation d'une conférence internationale de premier plan fut un projet colossal, qui s'est ajouté à une charge de travail déjà lourde. Je suis aussi contente que notre Commissariat attire une nouvelle génération d'experts dans le domaine des renseignements personnels.

Je tiens à remercier tous les employés du Commissariat à la protection de la vie privée pour leur contribution immense dans les efforts visant à préserver le droit à la protection de la vie privée des Canadiennes et Canadiens.

Jennifer Stoddart

Commissaire à la protection de la vie privée du Canada

Le groupe a produit un rapport résumant les pouvoirs que détiennent les autorités d'exécution de la loi dans les pays membres de l'OCDE et leur capacité de partager des renseignements pour faciliter la coopération transfrontalière. D'après ce rapport, en dépit des différences dans les lois nationales, il reste beaucoup de latitude pour adopter une approche plus mondiale et systématique en matière de coopération transfrontalière dans l'application des lois visant à protéger la vie privée. En juin 2007, l'OCDE a adopté une recommandation sur la coopération transfrontalière basée sur le travail réalisé par le groupe de bénévoles.

On soulignera également le travail du groupe de bénévoles en juin 2008 lors d'une réunion ministérielle de l'OCDE en Corée où le thème sera l'avenir de l'économie du Net.

Le Commissariat a également participé au travail mené par la Coopération économique de la zone Asie-Pacifique (APEC) sur les questions relatives à la protection de la vie privée.

Le Canada s'est montré actif en veillant à ce que les règles de protection des données de l'APEC témoignent des valeurs et principes de base en matière de protection de la vie privée. Ces règles profiteront clairement aux Canadiennes et Canadiens étant donné le flux croissant de nos données échangées avec les pays membres de l'APEC. Notre travail en 2007 consistait à examiner des moyens de mettre en œuvre le cadre de protection de la vie privée créé par l'APEC.

## Réforme de la LPRPD

Ici au Canada, nous avons appuyé le travail d'un comité de députés chargés d'examiner la LPRPD. Les membres du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes ont présenté au gouvernement fédéral 25 recommandations visant à mettre au point la LPRPD. La recommandation qui a reçu le plus d'attention était celle qui faisait état d'une notification obligatoire des atteintes à la sécurité des données — un concept auquel j'adhère totalement.

En guise de réponse, le gouvernement fédéral a lancé tard dans l'année un processus de consultations publiques sur la réforme de la LPRPD, réclamant des opinions sur les paramètres relatifs aux notifications concernant les atteintes à la sécurité des données et sur d'autres questions.

Nous apprécions ces consultations et sommes impatients de voir les changements apportés à la LPRPD afin de l'améliorer — et d'assurer une protection encore plus grande de la vie privée des Canadiennes et Canadiens.

## Une préoccupation mondiale

Pour tout dire, l'incidence de la mondialisation sur la protection de la vie privée préoccupe de plus en plus le Commissariat. Le fait qu'une quantité grandissante de renseignements personnels traverse les frontières signifie que les atteintes à la protection des données touchent souvent des gens dans de multiples pays – comme ce fut le cas avec TJX/Winnex. La popularité croissante d'Internet soulève également de nombreuses questions transfrontalières qui ont des répercussions sur le Commissariat.

Je me réjouis d'annoncer que nous progressons dans notre travail auprès de nos homologues internationaux pour trouver des solutions mondiales à la protection de la vie privée.

Les résolutions adoptées durant la Conférence par les autorités de protection des données de tous les continents tenaient compte du contexte de plus en plus mondial des questions relatives à la protection de la vie privée.

Les commissaires ont réclamé des normes internationales concernant l'utilisation et la communication des renseignements personnels recueillis par un transporteur sur ses passagers. Ils ont affirmé que le transfert de renseignements personnels entre les agents de voyage, les transporteurs et les gouvernements nationaux et étrangers pose une menace constante à la protection de la vie privée des passagers. Il faut trouver une solution mondiale en collaboration avec les transporteurs, les organismes d'application de la loi, les organismes internationaux, les groupes de défense des libertés civiles ainsi que les experts en protection des données et de la vie privée.

Les autorités de protection des données ont adopté deux autres résolutions : 1) améliorer la coopération internationale; 2) mettre à profit le travail réalisé par l'Organisation internationale de normalisation pour établir des normes communes en matière de protection de la vie privée dans le domaine de la technologie de l'information.

Le Commissariat s'intéresse également aux questions transfrontalières dans le cadre d'autres initiatives internationales.

## Efforts de l'OCDE et de l'APEC

Je suis enchantée de présider un groupe de bénévoles de l'Organisation de coopération et de développement économiques (OCDE) dont le but est d'encourager la coopération entre les autorités de protection des données et d'autres organismes d'application de la loi en ce qui a trait aux plaintes transfrontalières et aux affaires découlant de la circulation transfrontalière des données.



Notre orateur principal était le secrétaire à la sécurité intérieure des États-Unis, Michael Chertoff, qui n'a pas mis de gants blancs pour faire valoir ses opinions sur l'équilibre à atteindre en matière de droit à la protection de la vie privée dans le contexte de la sécurité nationale, devant un auditoire quelque peu sceptique — ce qui a provoqué beaucoup de discussions durant toute la Conférence!

Un membre de notre Comité consultatif externe, Michael Geist, professeur de droit à l'Université d'Ottawa, qui est titulaire de la Chaire de recherche du Canada en droit d'Internet et du commerce électronique, a plus tard réagi en décrivant devant des centaines de défenseurs du droit à la vie privée l'approche de Chertoff axée sur une surveillance accrue par les gouvernements comme étant un « défi conflictuel ».

« ... Sa vision d'une société sous surveillance générale — appuyée par des bases de données biométriques massives recueillies de centaines de millions de gens — est celle d'un futur qui donne froid dans le dos. Plutôt que *terra incognita*, Chertoff semblait dire qu'il existe une réalité connue quant au cours des choses à venir, et que le milieu de la protection de la vie privée ne peut y faire grand-chose », a écrit Geist sur son populaire blogue. [Traduction]

Avec un peu de chance, les commentateurs de Chertoff stimuleront les défenseurs du droit à la vie privée à plaider encore plus fermement en faveur du droit à la vie privée en cette ère de l'après-11 septembre.

Le programme de la Conférence mettrait en relief le vaste éventail d'enjeux qui auront une incidence sur la protection de la vie privée dans les années à venir ainsi que la nature de plus en plus mondiale des questions de protection de la vie privée.

Nous avons préparé 14 cahiers de consultation avant la Conférence. La plupart incluaient un document commandé à un expert en la matière et diverses autres ressources, comme du matériel bibliographique, pour satisfaire la curiosité des participants qui peuvent être des profanes dans un domaine particulier, ainsi que les exigences plus rigoureuses des principaux décideurs pour repérer l'information fiable concernant les répercussions sur la vie privée des thèmes abordés lors de la Conférence. Ces cahiers sont accessibles le site Web de notre conférence à [www.privacyconference2007.gc.ca](http://www.privacyconference2007.gc.ca) et constituent un legs important de la Conférence.

Nous avons affiché les détails du coût de la Conférence sur notre site Web. Nous sommes bien à l'intérieur de nos objectifs financiers.

Les participants ont fait des commentaires extrêmement positifs. En fait, une des rares frustrations exprimées par les délégués concernait le fait qu'il y avait trop de séances intéressantes qui se produisaient en même temps!

Nous avons accueilli plus de 600 commissaires, universitaires, spécialistes de la protection de la vie privée, défenseurs des droits, responsables gouvernementaux, spécialistes de la TI, etc., de partout dans le monde – ce qui en fit la plus grande conférence du genre jamais organisée. Par-dessus tout, les critiques positives et les félicitations que nous avons reçues de la part des participants ont justifié le temps et les ressources investis dans cet événement.

Le thème de la Conférence était « Les horizons de la protection de la vie privée : *Terra incognita* ». Les anciens cartographes utilisaient ce mot latin pour désigner les territoires inconnus qu'il restait à délimiter sur une carte. Sur l'un des premiers globes terrestres connus de l'Europe, on peut lire sur un bord non cartographié de l'océan « *hic sunt dracones* », ce qui veut dire « Ici résident les dragons ».

La notion de paysage inconnu avec des dragons qui rôdent semblait la métaphore parfaite pour l'avvenir de la protection de la vie privée.

Les enjeux relatifs à la protection de la vie privée changent rapidement; l'arrivée de puissantes nouvelles technologies et la guerre internationale au terrorisme agissant comme forces pouvant menacer la vie privée des gens autour du monde.

Le but de notre conférence était de commencer à brosser un tableau de ce à quoi le pourrait ressembler demain le monde de la protection de la vie privée et aussi d'équiper les défenseurs du droit à la vie privée de quelques solides instruments pour tuer les dragons.

Durant une série de plénnières, d'ateliers et de séances d'information, nous avons examiné les meilleures stratégies par lesquelles défendre le droit à la protection de la vie privée dans un contexte de changements constants.

Les participants ont entendu les grands noms de la protection de la vie privée, y compris : Bruce Schneier, gourou en technologie de la sécurité et auteur, Simon Davies, pionnier sur la scène internationale de la protection de la vie privée et fondateur de Privacy International, Katharine Albrecht, défenseur de la vie privée des consommateurs; Marc Rotenberg, directeur exécutif du Electronic Privacy Information Center; Peter Fleischer, conseiller en matière de protection internationale des renseignements personnels pour Google; Peter Hustinx, contrôleur européen de la protection des données; Peter Schar, président sortant du Groupe de travail sur la protection des données établi en vertu de l'article 29 de l'UE; enfin, Alex Türk, de la France, qui assume actuellement la présidence du Groupe.

Notre invité d'honneur, sur place pour aider à lancer la Conférence, était l'honorable Peter Milliken, président de la Chambre des communes.

personnelles qu'elles recueillent. Cependant, il arrive trop souvent que des atteintes à la sécurité des données se produisent par suite d'une erreur humaine ou d'une approche cavalière en matière de sécurité.

Le Commissariat travaille avec le milieu des affaires au Canada pour améliorer les pratiques en matière de protection de la vie privée et encourager le recours à des mesures de sécurité solides en matière de technologie de l'information.

Les récentes manchettes sur des atteintes importantes à la sécurité des données amènent également les entreprises à revoir la façon dont elles gèrent la protection de la vie privée et la sécurité. Aucune entreprise ne souhaite avoir à appeler ses clients pour leur apprendre qu'il y a eu fuite de leurs renseignements personnels.

Je souhaite que 2008 marque un point tournant dans la protection des renseignements personnels. Il est temps que les entreprises reconnaissent la valeur de tels renseignements – et la nécessité de les protéger adéquatement.

Malheureusement, le défi que pose la sauvegarde des renseignements personnels est plus grand que jamais. La quantité de données personnelles recueillies, stockées et partagées ne cesse de croître – tout comme l'ingéniosité des fraudeurs et des pirates.

## Une année chargée

Le Commissariat se souviendra également que 2007 fut l'année où nous avons :

- organisé la 29<sup>e</sup> Conférence internationale des commissaires à la protection des données et de la vie privée;
- élargi la portée de notre travail sur la scène internationale;
- participé aux efforts pour améliorer la *LPRPDE*;
- accueilli une nouvelle commissaire adjointe.

Voici maintenant quelques réflexions sur chacun de ces événements et sur les enjeux clés de l'année.

## Organisation de la Conférence mondiale

Le succès de la 29<sup>e</sup> Conférence internationale des commissaires à la protection des données et de la vie privée – qui s'est déroulée à Montréal en septembre et faisait suite à notre engagement pris en 2002 – a dépassé nos attentes les plus élevées.

On se souviendra sans nul doute de l'année 2007 dans le monde de la protection de la vie privée comme de l'année de l'atteinte à la sécurité des données.

La taille de certaines fuites de données recensées sur la planète était ahurissante : l'irruption de pirates informatiques dans le système de TJX Companies Inc., le géant du détail américain propriétaire des magasins Winners et HomeSense au Canada, a mis à découvert environ 94 millions de cartes de crédit et de débit. Au Royaume-Uni, deux disques informatiques contenant les données personnelles de quelque 25 millions de particuliers touchant des prestations pour enfants ont disparu.

Il ne s'agit là que des deux désastres les plus médiatisés en matière de sécurité des données. On a également appris qu'il était survenu un grand nombre d'autres atteintes à la sécurité des données qui ont touché des millions de gens partout dans le monde.

Chez nous, au Canada, les atteintes à la sécurité des données ont tenu notre équipe extraordinairement occupée en 2007.

Nous avons notamment fait enquête sur l'accès non autorisé aux données de TJX/Winners ainsi que sur la disparition d'un disque dur contenant les renseignements personnels de près d'un demi-million de clients des fonds communs de placement Talvest, une filiale de la Banque canadienne impériale de commerce (CIBC).

## Une obligation pour les entreprises

Il va de soi que les organisations de toutes tailles peuvent – et doivent – en faire davantage pour prévenir les fuites de données.

Selon la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), les entreprises sont tenues de préserver adéquatement les données







# TABLE DES MATIÈRES

Message de la commissaire .....	1
La protection de la vie privée en chiffres en 2007.....	9
Nouvelles priorités stratégiques.....	11
Principales réalisations en 2007.....	15
Enjeu clé : Atteintes à la sécurité des données.....	19
Enquête sur une atteinte à la sécurité des données : L'affaire TJX.....	24
Manière dont le Commissariat aide les organisations à prévenir les atteintes à la sécurité des données.....	27
Amélioration de la LPRPD .....	29
Enquêtes sur les plaintes et demandes de renseignements .....	33
Vérification et revue .....	47
Devant les tribunaux .....	51
Lois provinciales et territoriales essentiellement similaires .....	61
L'année qui vient .....	63
Annexe 1 – Définitions; processus d'enquête.....	65
Définitions des types de plaintes déposées en vertu de la LPRPD.....	65
Définitions des conclusions et d'autres dispositions .....	66
Processus d'enquête en vertu de la LPRPD .....	68
Annexe 2 – Statistiques en matière d'enquête et de demandes de renseignements .....	71
Demandes de renseignements en vertu de la LPRPD reçues.....	71
Demandes de renseignements en vertu de la LPRPD réglées.....	71
Plaintes reçues par type de plainte.....	72
Plaintes reçues – Répartition par secteur .....	73
Plaintes résolues par type de plainte .....	74
Plaintes résolues par type de conclusion .....	75
Délais de traitement des enquêtes en vertu de la LPRPD .....	76
– Par type de conclusion .....	76
Conclusions par type de plainte.....	77
Conclusions par secteur industriel .....	78
Délais de traitement des enquêtes en vertu de la LPRPD – Par type de plainte .....	79



**Commissionnaire à la protection  
de la vie privée du Canada**  
**Privacy Commissioner  
of Canada**

112, rue Kent  
Ottawa (Ontario)  
K1A 1H3  
Tél. : (613) 995-8210  
Téléc. : (613) 947-6850  
www.privcom.gc.ca

112 Kent Street  
Ottawa, Ontario  
K1A 1H3  
Tél. : (613) 995-8210  
Fax : (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca



Juin 2008

L'honorable Peter Milliken, député  
Président  
Chambre des communes  
Ottawa (Ontario) K1A 0A6  
Monsieur,

J'ai l'honneur de présenter au Parlement le rapport annuel sur la *Loi sur la protection des renseignements personnels et les documents électroniques* du Commissariat à la protection de la vie privée du Canada pour la période s'échelonnant du 1<sup>er</sup> janvier au 31 décembre 2007.

Veuillez agréer, Monsieur, l'assurance de ma considération distinguée.

La commissaire à la protection  
de la vie privée du Canada,

*Jennifer Stoddart*  
Jennifer Stoddart





Juin 2008

L'honorable Noël A. Kinsella, sénateur  
Président  
Sénat du Canada  
Ottawa  
Monsieur,

J'ai l'honneur de présenter au Parlement le rapport annuel sur la *Loi sur la protection des renseignements personnels et les documents électroniques* du Commissariat à la protection de la vie privée du Canada pour la période s'échelonnant du 1<sup>er</sup> janvier au 31 décembre 2007.

Veuillez agréer, Monsieur, l'assurance de ma considération distinguée.

La commissaire à la protection  
de la vie privée du Canada,

*Jennifer Stoddart*

Jennifer Stoddart



Commissariat à la protection de la vie privée du Canada  
112, rue Kent  
Ottawa (Ontario) K1A 1H3

613-995-8210, 1-800-282-1376

Téléc. : 613-947-6850

ATS : 613-992-9190

© Ministère des Travaux publics et Services gouvernementaux Canada 2008

N° de cat. : IP51-1/2007

ISBN : 978-0-662-05757-4

Cette publication se trouve également sur notre site Web à [www.privcom.gc.ca](http://www.privcom.gc.ca).



Rapport sur la  
Loi sur la protection des  
renseignements personnels  
et les documents électroniques

2007

RAPPORT ANNUEL AU PARLEMENT

Vie Privée

Privacy Commissioner  
of Canada



Commissaire à la protection  
de la vie privée du Canada

3269



Commissaire à la protection  
de la vie privée du Canada



Privacy Commissioner  
of Canada

# Vie Privée

## RAPPORT ANNUEL AU PARLEMENT

# 2007

Rapport sur la  
Loi sur la protection des  
renseignements personnels  
et les documents électroniques













